VALKYRIE COMODO

Summary

File Name: MediaPlay_id3754771id.exe

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

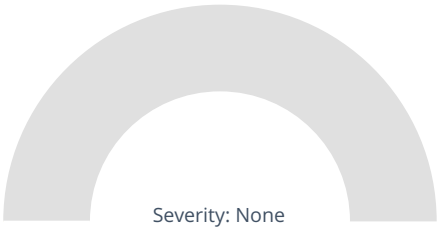
SHA1: 4618f1ae573e668331fa830efcc1c8050c23eff1

MD5: 786bdcc6f403a6bde9ef002e19e391ac

CLEAN

Valkyrie Final Verdict

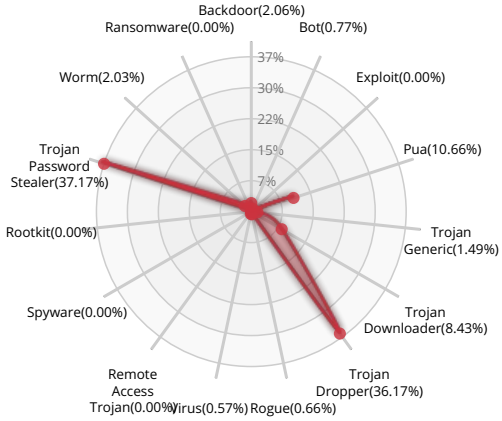
DETECTION SECTION



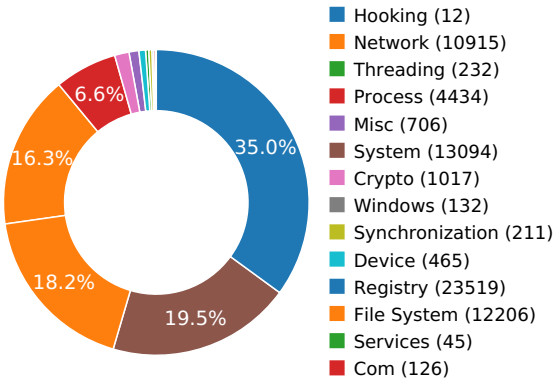
Severity: None

Verdict: Clean

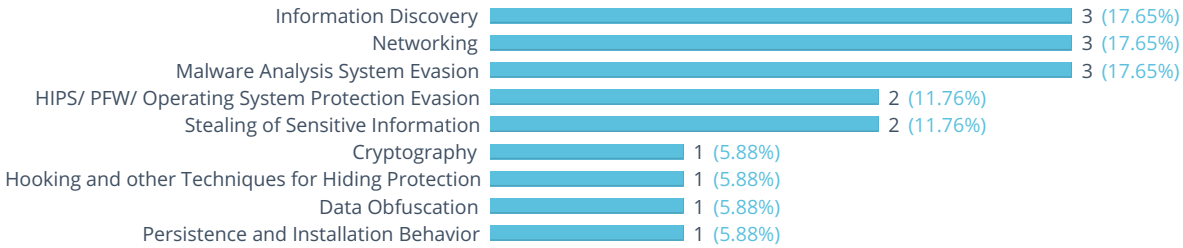
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources
Repeatedly searches for a not-found process, may want to run with startbrowser=1 option	
Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (10 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory	Show sources
Attempts to identify installed AV products by registry key	Show sources

CRYPTOGRAPHY

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

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources
Attempts to modify proxy settings	

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a file	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

06:12:29 **06:15:44** **06:18:58**

PID 1636

06:12:29 **Create Process** The malicious file created a child process as 4618f1ae573e668331fa830efcc1c8050c23eff1.exe **(PPID 1760)**

06:12:29 VirtualProtectEx

06:12:29 06:12:29 NtReadFile **[4 times]**

06:12:30 Create Process

PID 2560

06:12:30 **Create Process** The malicious file created a child process as 4618f1ae573e668331fa830efcc1c8050c23eff1.tmp **(PPID 1636)**

06:12:35 RegOpenKeyExW

06:14:09 06:14:09 NtReadFile **[52 times]**

06:14:52 Create Process

06:15:05 06:15:07 ConnectEx **[2 times]**

PID 1152

06:14:54 **Create Process** The malicious file created a child process as netsh.exe **(PPID 2560)**

PID 2176

06:12:32 **Create Process** The malicious file created a child process as homepage.exe **(PPID 2560)**

06:12:32 06:12:32 NtReadFile **[2 times]**

PID 1504

06:14:19 **Create Process** The malicious file created a child process as 7z.exe **(PPID 2560)**

PID 1588

06:14:23 **Create Process** The malicious file created a child process as 7z.exe **(PPID 2560)**

PID 2780

06:14:24 **Create Process** The malicious file created a child process as mediaplay-vbm.exe **(PPID 2560)**

06:14:25 06:14:26 ConnectEx **[2 times]**

06:14:27 06:14:27 NtReadFile **[11 times]**

06:14:27 06:14:27 Process32NextW **[3 times]**

06:14:27 ConnectEx

06:15:10 06:15:11 NtQueryFullAttributesF **[48 times]**

06:15:12 NtQueryAttributesFile

06:15:12 NtCreateFile

06:15:13 06:15:14 NtQueryFullAttributesF **[72 times]**

06:15:28 06:15:29 Process32NextW [6 times]

06:15:29 06:15:29 NtReadFile [5 times]

06:15:30 06:15:30 ConnectEx [2 times]

06:15:35 RegSetValueExW

06:15:35 06:15:35 Process32NextW [2 times]

06:15:35 Create Process

06:15:43 ConnectEx

06:15:46 Process32FirstW

06:15:46 06:15:46 NtReadFile [2 times]

06:15:48 Process32NextW

06:15:48 NtSetInformationFile

06:16:08 06:18:58 Process32FirstW [3 times]

06:18:58 06:18:58 NtReadFile [8 times]

PID 2692

06:15:20 **Create Process** The malicious file created a child process as na_runner.exe **(PPID 2780)**

06:15:21 Process32FirstW

06:15:21 NtCreateFile

06:15:21 06:15:21 Process32NextW [2 times]

06:15:21 NtCreateFile

06:15:21 RegSetValueExW

06:15:21 ConnectEx

06:15:27 Create Process

06:15:27 CreateServiceW

06:15:31 Process32NextW

PID 2356

06:15:27 **Create Process** The malicious file created a child process as MailRuUpdater.exe **(PPID 2692)**

06:15:28 06:15:28 Process32FirstW [2 times]

06:15:28 06:15:28 ConnectEx [4 times]

06:15:30 Process32NextW

06:15:30 06:15:30 Process32FirstW [2 times]

06:15:30 06:15:30 NtReadFile [5 times]

06:15:30 Process32NextW

06:15:30 Process32FirstW

06:15:30 [2 times]

06:15:30 06:15:30 NtReadFile [2 times]

06:15:30 Process32NextW

06:15:31 Process32FirstW

06:15:31 Process32NextW

06:15:31 06:15:56 Process32FirstW [3 times]

06:18:08 Process32NextW

06:18:08 ConnectEx

PID 2904

06:14:24 **Create Process** The malicious file created a child process as mediaplay-a.exe **(PPID 2560)**

06:14:24 Create Process

PID 2388

06:14:24 **Create Process** The malicious file created a child process as mediaplay-a.exe **(PPID 2904)**

06:14:30 06:14:31 ConnectEx [3 times]

06:14:33 NtSetInformationFile

PID 1160

06:18:48 **Create Process** The malicious file created a child process as mediaplay-a.exe **(PPID 2388)**

PID 872

06:15:23 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

PID 460

06:15:28 **Create Process** The malicious file created a child process as services.exe **(PPID 352)**

06:15:30 Create Process

06:15:34 06:17:58 GetSystemTimeAsFileTi [10 times]

PID 228

06:15:30 **Create Process** The malicious file created a child process as MailRuUpdater.exe **(PPID 460)**

06:15:31 Process32FirstW

06:15:31 06:15:32 ConnectEx [3 times]

06:15:33 Process32FirstW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.ENU
C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.ENU.DLL
C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.EN
C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.EN.DLL
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.ENU
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.ENU.DLL
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.EN
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.EN.DLL
\Device\KsecDD
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.ENU
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.ENU.DLL
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.EN
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.EN.DLL
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.tmp.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

c:\directory
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mail_logo.bmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\Microsoft.VC90.CRT.manifest
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\msvcm90.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\msvcp90.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\msvcr90.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\homepage.exe
C:\Windows\System32\en-US\msxml3r.dll.mui
\??\MountPointManager
C:\Windows\SysWOW64\wininet.dll
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies
C:\Users\user\AppData\Local\Microsoft\Windows\History
C:\Users\user\AppData\Local\Microsoft\Windows\History\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\iphlpapi.DLL
C:\Windows\System32\IPHLPAPI.DLL
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\WINNSI.DLL
C:\Windows\System32\winnsi.dll
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk

C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-part1.7z
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-a.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-vbm.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.dll
C:\
C:\Windows\System32
C:\Users\user\AppData\Local\MediaPlay

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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
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\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\itdownload.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Client\(Default)
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\FromCacheTimeout
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CertificateRevocation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableKeepAlive
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisablePassport
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\IdnEnabled
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CacheMode
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableNegotiate
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableBasicOverClearChannel
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\Feature_ClientAuthCertFilter

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mail_logo.bmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\Microsoft.VC90.CRT.manifest
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\msvcm90.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\msvcp90.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\msvcr90.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\homepage.exe
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-part1.7z

C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-a.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-vbm.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.dll
C:\Users\user\AppData\Local\MediaPlay\unins000.dat
C:\Users\user\AppData\Local\MediaPlay\is-3GQAL.tmp
C:\Users\user\AppData\Local\MediaPlay\unins000.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\is-OLTR5.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\yandex-dummy.txt
\??\PIPE\srvsvc
C:\Users\Public\Desktop\MediaPlay.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\MediaPlay.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\MediaPlay.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\Uninstall.lnk
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\Local\Temp\Cab8C78.tmp
C:\Users\user\AppData\Local\Temp\Tar8C79.tmp
C:\Users\user\AppData\Local\MediaPlay\Firefox\chrome.manifest
C:\Users\user\AppData\Local\MediaPlay\Microsoft.VC90.CRT.manifest
C:\Users\user\AppData\Local\MediaPlay\imageformats\Microsoft.VC90.CRT.manifest
C:\Users\user\AppData\Local\MediaPlay\Firefox\chrome\content\mg_ffext.js
C:\Users\user\AppData\Local\MediaPlay\Firefox\install.rdf
C:\Users\user\AppData\Local\MediaPlay\Firefox\components\img_ffext.xpt
C:\Users\user\AppData\Local\MediaPlay\Firefox\chrome\content\mg_ffext.xul
C:\Users\user\AppData\Local\MediaPlay\mediaplay.exe
C:\Users\user\AppData\Local\MediaPlay\libeay32.dll
C:\Users\user\AppData\Local\MediaPlay\libtcmalloc_minimal.dll
C:\Users\user\AppData\Local\MediaPlay\libvlc.dll
C:\Users\user\AppData\Local\MediaPlay\libvlccore.dll
C:\Users\user\AppData\Local\MediaPlay\MediaInfo.dll
C:\Users\user\AppData\Local\MediaPlay\Firefox\components\mg_ffext.dll
C:\Users\user\AppData\Local\MediaPlay\msvcm90.dll
C:\Users\user\AppData\Local\MediaPlay\msvcp90.dll

C:\Users\user\AppData\Local\MediaPlay\msvcr90.dll

C:\Users\user\AppData\Local\MediaPlay\imageformats\qgif4.dll

C:\Users\user\AppData\Local\MediaPlay\imageformats\qjpeg4.dll

C:\Users\user\AppData\Local\MediaPlay\imageformats\qmng4.dll

C:\Users\user\AppData\Local\MediaPlay\QtCore4.dll

C:\Users\user\AppData\Local\MediaPlay\QtDeclarative4.dll

C:\Users\user\AppData\Local\MediaPlay\QtGui4.dll

C:\Users\user\AppData\Local\MediaPlay\QtNetwork4.dll

C:\Users\user\AppData\Local\MediaPlay\QtScript4.dll

C:\Users\user\AppData\Local\MediaPlay\QtSql4.dll

C:\Users\user\AppData\Local\MediaPlay\QtXml4.dll

C:\Users\user\AppData\Local\MediaPlay\QtXmlPatterns4.dll

C:\Users\user\AppData\Local\MediaPlay\ssleay32.dll

C:\Users\user\AppData\Local\MediaPlay\Firefox\components\.autoreg

C:\Users\user\AppData\Local\MediaPlay\imageformats

C:\Users\user\AppData\Local\MediaPlay\Firefox\components

C:\Users\user\AppData\Local\MediaPlay\Firefox\chrome\content

C:\Users\user\AppData\Local\MediaPlay\Firefox\chrome

C:\Users\user\AppData\Local\MediaPlay\Firefox

C:\ProgramData\Mail.Ru\Id

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm

C:\Users\user\AppData\Local\Temp\4e4b-88ac-a320-f61b\MailRu.ico

C:\Users\user\AppData\Local\Mail.Ru\Sputnik\MailRu.ico

C:\Users\user\AppData\Local\Temp\70c7-5033-39a6-2a48\GoMailRu.ico

C:\Users\user\AppData\Local\Mail.Ru\Sputnik\GoMailRu.ico

RESOLVED APIS

kernel32.dll.SetDllDirectoryW

kernel32.dll.SetSearchPathMode

kernel32.dll.SetProcessDEPPolicy

kernel32.dll.GetDiskFreeSpaceExW

kernel32.dll.Wow64DisableWow64FsRedirection

kernel32.dll.Wow64RevertWow64FsRedirection
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
kernel32.dll.GetUserDefaultUILanguage
comctl32.dll.RegisterClassNameW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled
uxtheme.dll.EnableThemeDialogTexture
kernel32.dll.InitializeConditionVariable
kernel32.dll.WakeConditionVariable
kernel32.dll.WakeAllConditionVariable
kernel32.dll.SleepConditionVariableCS

user32.dll.WINNLSEnableIME
imm32.dll.ImmGetContext
imm32.dll.ImmReleaseContext
imm32.dll.ImmGetConversionStatus
imm32.dll.ImmSetConversionStatus
imm32.dll.ImmSetOpenStatus
imm32.dll.ImmSetCompositionWindow
imm32.dll.ImmSetCompositionFontW
imm32.dll.ImmGetCompositionStringW
imm32.dll.ImmIsIME
imm32.dll.ImmNotifyIME
user32.dll.GetMonitorInfoA
user32.dll.GetSystemMetrics
user32.dll.EnumDisplayMonitors
cryptbase.dll.SystemFunction036
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

DELETED FILES

C:\Users\user\AppData\Local\MediaPlay\is-3GQAL.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\is-OLTR5.tmp
C:\Users\Public\Desktop\MediaPlay.lnk
C:\Users\Public\Desktop\MediaPlay.pif
C:\Users\Public\Desktop\MediaPlay.url
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\MediaPlay.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\MediaPlay.pif
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\MediaPlay.url
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\MediaPlay.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\MediaPlay.pif
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\MediaPlay.url
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\Uninstall.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\Uninstall.pif
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\Uninstall.url
C:\Users\user\AppData\Local\Temp\Cab8C78.tmp
C:\Users\user\AppData\Local\Temp\Tar8C79.tmp
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal
C:\Users\user\AppData\Local\Temp\4e4b-88ac-a320-f61b\MailRu.ico
C:\Users\user\AppData\Local\Temp\4e4b-88ac-a320-f61b
C:\Users\user\AppData\Local\Temp\70c7-5033-39a6-2a48\GoMailRu.ico
C:\Users\user\AppData\Local\Temp\70c7-5033-39a6-2a48
C:\Users\user\AppData\Local\Temp\64f2-798a-6964-0384
C:\Users\user\AppData\Local\Temp\e45e-9fa6-6843-8bb8\na_runner.exe
C:\Users\user\AppData\Local\Temp\e45e-9fa6-6843-8bb8
C:\Users\user\AppData\Local\Temp\dc3e-9e83-da0d-a1c8\gbnhehnpnbiioheicppmmmjaekcdfigc\manifest.json
C:\Users\user\AppData\Local\Temp\dc3e-9e83-da0d-a1c8\gbnhehnpnbiioheicppmmmjaekcdfigc
C:\Users\user\AppData\Local\Temp\dc3e-9e83-da0d-a1c8
C:\Users\user\AppData\Local\Temp\3167-b30a-014e-e4c0\fppjhfcgnalgfiimdflmikpifodndljf\manifest.json
C:\Users\user\AppData\Local\Temp\3167-b30a-014e-e4c0\fppjhfcgnalgfiimdflmikpifodndljf
C:\Users\user\AppData\Local\Temp\3167-b30a-014e-e4c0

C:\Users\user\AppData\Local\Temp\dfba-ffdd-126c-b693\ebkgajjadgojjkgacfgjpnpgagpecpjp\manifest.json
C:\Users\user\AppData\Local\Temp\dfba-ffdd-126c-b693\ebkgajjadgojjkgacfgjpnpgagpecpjp
C:\Users\user\AppData\Local\Temp\dfba-ffdd-126c-b693
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences_d9a7-491c-ef9e-d75f
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences_405d-ef92-b996-0853
C:\Users\user\AppData\Local\Temp\ff9a-03f3-40ab-d77b\mail_16.png
C:\Users\user\AppData\Local\Temp\ff9a-03f3-40ab-d77b
C:\Users\user\AppData\Local\Temp\mini_loader_scoped_dir_1535188497\mediaplay-a.exe.dul!
C:\Users\user\AppData\Local\Temp\mini_loader_scoped_dir_1535188497\mediaplay-a.exe
C:\Windows\Tasks\MailRuUpdater.job
C:\Windows\SoftwareDistribution\DataStore\Logs\edbtmp.log

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
HKEY_CURRENT_USER\Software\Mail.Ru\Tech\dfrrdsks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\MailRuUpdater.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\MailRuUpdater.job.fp
HKEY_CURRENT_USER\Software\Mail.Ru\SicSettings

REGISTRY KEYS

HKEY_CURRENT_USER\Software\CodeGear\Locales
HKEY_LOCAL_MACHINE\Software\CodeGear\Locales
HKEY_CURRENT_USER\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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
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\System\CurrentControlSet\Control\Keyboard Layouts\04090409
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\4618f1ae573e668331fa830efcc1c8050c23eff1.tmp
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\itdownload.dll
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Sans Serif
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Verdana
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software
HKEY_LOCAL_MACHINE\Software
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.tmp" /SL5="$A0162,1296912,154112,C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.exe"
"C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\homepage.exe" C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\homepage.txt
"C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.exe" x -y -o"C:\Users\user\AppData\Local\MediaPlay" "C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-part1.7z"

"C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.exe" x -y -o"C:\Users\user\AppData\Local\Temp\is-47I4P.tmp" "C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-part2.7z"
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-vbm.exe /silent /rfr=mediaplay
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-a.exe --silent --rfr=mediaplay --ua_rfr=CHANNEL_mediaplay
C:\Users\user\AppData\Local\Amigo\Application\amigo.exe
"C:\Windows\System32\netsh.exe" firewall add allowedprogram program="C:\Users\user\AppData\Local\MediaPlay\mediaplay.exe" name=MediaPlay
netsh firewall add allowedprogram program="C:\Users\user\AppData\Local\MediaPlay\mediaplay.exe" name=MediaPlay
"C:\Users\user\AppData\Local\Temp\e45e-9fa6-6843-8bb8\na_runner.exe" --install
C:\Users\user\AppData\Local\Temp\loader_ldir_2904_30127\mediaplay-a.exe --silent --rfr=mediaplay --ua_rfr=CHANNEL_mediaplay --cp
"C:\Users\user\AppData\Local\Mail.Ru\MailRuUpdater.exe"
C:\Program Files (x86)\Mail.Ru\MailRuUpdater\MailRuUpdater.exe --s

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\4618f1ae573e668331fa830efcc1c8050c23eff1.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\itdownload.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\Windows\System32\en-US\msxml3r.dll.mui
C:\Windows\SysWOW64\wininet.dll
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-part1.7z
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-a.exe
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\mediaplay-vbm.exe

C:\
C:\Users\user\AppData\Local\MediaPlay\unins000.dat
C:\Windows\winsxs\FileMaps\users_user_appdata_local_mediaplay_0d369d03e557252d.cdf-ms
C:\Users\user\AppData\Local\MediaPlay\is-3GQAL.tmp
C:\Users\user\AppData\Local\Temp\is-OP7S1.tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.tmp
C:\Windows\winsxs\FileMaps\users_user_appdata_local_temp_is-47i4p.tmp_b4f2bdfb018dbaaf.cdf-ms
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\is-OLTR5.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\MediaPlay
\??\PIPE\srvsvc
C:\Users\user\AppData\Local\MediaPlay\mediaplay.exe
C:\Users\Public\Desktop\MediaPlay.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\MediaPlay.lnk
C:\Users\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\MediaPlay.lnk
C:\Users\user\AppData\Local\MediaPlay\unins000.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MediaPlay\Uninstall.lnk
C:\Windows\SysWOW64\ieframe.dll
C:\Windows
C:\Windows\System32
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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\Local\Temp\Cab8C78.tmp
C:\Users\user\AppData\Local\Temp\Tar8C79.tmp
C:\Windows\System32\en-US\winhttp.dll.mui
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs.js
C:\Users\user\AppData\Local\Temp\is-47I4P.tmp\7z.dll

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
DefaultTabtip-MainUI
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
0FB3B0CE-9638-4F8A-BE5C-EA9DBFA8FB0B
51483A5C-8B6C-4B66-8FE3-BAF0E3ACC997ch
MINI_LOADER_V2
IESQMMUTEX_0_208

C5024C9E-B935-480E-BB8C-23A23252E884-WM
Global\REMOTE_TASK_MUTEX
DBWinMutex

MODIFIED REGISTRY KEYS

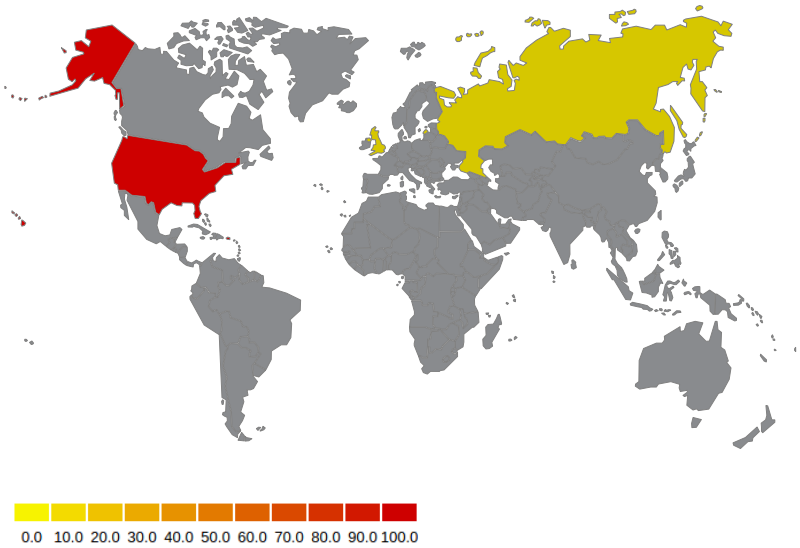
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\4618f1ae573e668331fa830efcc1c8050c23eff1_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\Inno Setup: Setup Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\Inno Setup: App Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\InstallLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\Inno Setup: Icon Group
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\Inno Setup: User
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\Inno Setup: Language
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\DisplayIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\UninstallDataFile
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\QuietUninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\DisplayVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\Publisher
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\URLInfoAbout

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\HelpLink
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\URLUpdateInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\NoModify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\NoRepair
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\MajorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\MinorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{6F13A0A9-4BC2-4750-8718-7B33663FE07F}}_is1\EstimatedSize
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Mail.Ru\Tech
HKEY_CURRENT_USER\Software\Mail.Ru\Tech\UserID
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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesResolve
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\Favorites
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAssocChangedCounter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\mailruhomesearch
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{5F87CBD4-C687-4AF5-A56A-69AA93BE36E9}User
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{5F87CBD4-C687-4AF5-A56A-69AA93BE36E9}Machine
HKEY_LOCAL_MACHINE\Software\Google\Chrome\Extensions\gbnhehnpnbiioheicppmmmjaekcdfigc
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\gbnhehnpnbiioheicppmmmjaekcdfigc\update_url
HKEY_LOCAL_MACHINE\Software\Google\Chrome\Extensions\fppjhfcgnalgfiimdflmikpifodndljf
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\fppjhfcgnalgfiimdflmikpifodndljf\update_url
HKEY_LOCAL_MACHINE\Software\Google\Chrome\Extensions\ebkgajjadgojjkgacfgjpnpgagpecpjp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\ebkgajjadgojjkgacfgjpnpgagpecpjp\update_url
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{B4D72CDC-3895-4C25-A969-8BD4FFC8B5D5}User
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{B4D72CDC-3895-4C25-A969-8BD4FFC8B5D5}Machine
HKEY_CURRENT_USER\Software\Mail.Ru\AmigoInstaller
HKEY_CURRENT_USER\Software\Mail.Ru\AmigoInstaller\LOADERGUID
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason

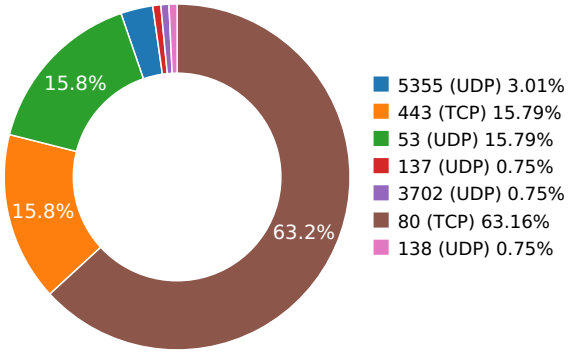
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-1
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-2
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-4
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-3
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-103

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
	151.101.2.133	United States	54113	Fastly	Malware Process
	23.215.131.177	United States	20940	Akamai Technologies, Inc.	OS Process
	23.215.131.194	United States	20940	Akamai Technologies, Inc.	OS Process
	23.215.131.200	United States	20940	Akamai Technologies, Inc.	OS Process
xmlbinupdate.mail.ru	217.69.139.247	Russian Federation	47764		Malware Process
binupdate.mail.ru	217.69.139.245	Russian Federation	47764		Malware Process
crl.microsoft.com	208.185.118.90	United States	6461	Zayo Bandwidth	OS Process
mrds.mail.ru	217.69.139.245	Russian Federation	47764		Malware Process
crl.globalsign.net	151.101.22.133	United States	54113	Fastly	Malware Process
sputnikmailru.cdnmail.ru	217.69.139.110	Russian Federation	47764		Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Servic...	Malware Process
download.mediaplay.ru	193.0.201.76	Russian Federation	14576		Malware Process
status.geotrust.com	72.21.91.29	United States	15133	MCI Communications Servic...	Malware Process
xtnmailru.cdnmail.ru	217.69.139.110	Russian Federation	47764		Malware Process
amigobin.cdnmail.ru	217.69.139.110	Russian Federation	47764		Malware Process
ctldl.windowsupdate.com	208.185.118.90	United States	6461	Zayo Bandwidth	OS Process
conserv.go.mail.ru	217.69.139.122	Russian Federation	47764		Malware Process
mailruupdater.cdnmail.ru	217.69.139.110	Russian Federation	47764		Malware Process
goappsdl.distribmail.ru	217.69.139.110	Russian Federation	47764		Malware Process
install.mediaplay.ru	193.0.201.76	Russian Federation	14576		Malware Process
gosoftdl.mail.ru	217.69.139.110	Russian Federation	47764		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
download.mediaplay.ru	80	HEAD	1.0	InnoTools_Downloader	1	16.456859827
Path: /archives/mediaplay.7z **URI:** http://download.mediaplay.ru/archives/mediaplay.7z						
amigobin.cdnmail.ru	80	HEAD	1.0	InnoTools_Downloader	1	17.2857789993
Path: /AmigoDistrib.exe **URI:** http://amigobin.cdnmail.ru/AmigoDistrib.exe						
sputnikmailru.cdnmail.ru	80	HEAD	1.0	InnoTools_Downloader	1	18.4224359989
Path: /mailruhomesearchvbm.exe **URI:** http://sputnikmailru.cdnmail.ru/mailruhomesearchvbm.exe						
download.mediaplay.ru	80	GET	1.0	InnoTools_Downloader	1	18.7048649788
Path: /archives/mediaplay.7z **URI:** http://download.mediaplay.ru/archives/mediaplay.7z						
amigobin.cdnmail.ru	80	GET	1.0	InnoTools_Downloader	1	86.6489720345
Path: /AmigoDistrib.exe **URI:** http://amigobin.cdnmail.ru/AmigoDistrib.exe						
sputnikmailru.cdnmail.ru	80	GET	1.0	InnoTools_Downloader	1	91.2654488087
Path: /mailruhomesearchvbm.exe **URI:** http://sputnikmailru.cdnmail.ru/mailruhomesearchvbm.exe						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	115.154958963
Path: /update/2/version.txt?type=install&bgn=1&standalone=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=11&elapsed_time=0&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=install&bgn=1&standalone=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=11&elapsed_time=0&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	AmigoLoader	1	115.381068945
Path: /update/2/version.txt?GUID={BE6997F4-D488-4E58-BAAF-8DB21A213BEE}&os=6.1&type=mloader_run&newrfr=mediaplay **URI:** http://mrds.mail.ru/update/2/version.txt?GUID={BE6997F4-D488-4E58-BAAF-8DB21A213BEE}&os=6.1&type=mloader_run&newrfr=mediaplay						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	115.775806904
Path: /update/2/version.txt?type=spparams&raw=%2Fsilent%20%2Frfr%3Dmediaplay&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=11&elapsed_time=0&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=spparams&raw=%2Fsilent%20%2Frfr%3Dmediaplay&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=11&elapsed_time=0&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	117.681352854
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d5650b3dfa5fe814 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d5650b3dfa5fe814						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	118.372571945
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAVG%2Fhgj9%2BGUHaOfzhTEYXM%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAVG%2Fhgj9%2BGUHaOfzhTEYXM%3D						
status.geotrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	118.732784986
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR3enuod9bxDxzpICGW%2B2sabjf17QQUkFj%2FsJx1qFFUd7Ht8qNDFjiebMUCEAOWX413QS%2FkEIgesIUBbsM%3D **URI:** http://status.geotrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR3enuod9bxDxzpICGW%2B2sabjf17QQUkFj%2FsJx1qFFUd7Ht8qNDFjiebMUCEAOWX413QS%2FkEIgesIUBbsM%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	164.301146984
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	164.357324839
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	164.509754896
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	164.672330856
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	167.701465845
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?78d832fa9b32e377 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?78d832fa9b32e377						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	175.73230195
Path: /update/2/version.txt?type=setup_unit&id=taskbar_mailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=147&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=setup_unit&id=taskbar_mailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=147&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	176.344358921
Path: /update/2/version.txt?type=setup_unit&id=fav_gomailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=148&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=setup_unit&id=fav_gomailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=148&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	176.93561697

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /update/2/version.txt?type=setup_unit&id=ie_gomailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=148&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=setup_unit&id=ie_gomailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=148&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	177.457403898
Path: /update/2/version.txt?type=setup_unit&id=ie_mailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=149&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=setup_unit&id=ie_mailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=149&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	177.979858875
Path: /update/2/version.txt?type=setup_unit&id=desktop_mailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=149&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=setup_unit&id=desktop_mailru&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=149&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	181.860880852
Path: /update/2/version.txt?type=spnative_load&id=mrupdater&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=247&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=spnative_load&id=mrupdater&event=done&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=18&elapsed_time=247&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	184.287325859
Path: /update/2/version.txt?type=mru_install&ovr=0&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=7&elapsed_time=20&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=mru_install&ovr=0&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=0&comp_mem=3071&tool_mem=7&elapsed_time=20&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	190.596354961

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /update/2/version.txt?type=mru_online&tool=mrupdater&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=7&elapsed_time=21&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D **URI:** http://mrds.mail.ru/update/2/version.txt?type=mru_online&tool=mrupdater&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=7&elapsed_time=21&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	192.216838837
Path: /update/2/version.txt?type=task_executed&taskid=%7B901B414B-72A2-48C6-8DCD-29388B8B3E40%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=100&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7B901B414B-72A2-48C6-8DCD-29388B8B3E40%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=100&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	193.085071802
Path: /update/2/version.txt?type=task_executed&taskid=smon&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=101&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=smon&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=101&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	193.212225914
Path: /update/2/version.txt?type=sp_prep&time=165091&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=18&elapsed_time=314&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=sp_prep&time=165091&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=18&elapsed_time=314&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	193.560796022
Path: /update/2/version.txt?type=mru_online_service&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=7&elapsed_time=20&mr_service=1&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=mru_online_service&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=7&elapsed_time=20&mr_service=1&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	193.574321985

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /update/2/version.txt?type=mru_install_service&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=8&elapsed_time=31&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=mru_install_service&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=8&elapsed_time=31&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	193.716240883
Path: /update/2/version.txt?type=mruinfo&last_ch=80263646&ch_ver=48.0.2564.103&ie_hp=www.google.ro&ie_dse=www.bing.com&ie_ver=8.00.7600.16385&last_ff=46655904&ff_ver=46.0.1&asterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=693&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=mruinfo&last_ch=80263646&ch_ver=48.0.2564.103&ie_hp=www.google.ro&ie_dse=www.bing.com&ie_ver=8.00.7600.16385&last_ff=46655904&ff_ver=46.0.1&asterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=693&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	194.296264887
Path: /update/2/version.txt?type=task_executed&taskid=%7B2AB1F4AB-E3FA-4047-9033-EC223C8354F5%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=693&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7B2AB1F4AB-E3FA-4047-9033-EC223C8354F5%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=693&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	194.846709013
Path: /update/2/version.txt?type=task_executed&taskid=%7B4C1D0C36-25B2-4774-80E8-DAE1E7898A1A%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=1284&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7B4C1D0C36-25B2-4774-80E8-DAE1E7898A1A%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=11&elapsed_time=1284&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	194.872252941
Path: /update/2/version.txt?type=task_executed&taskid=%7B901B414B-72A2-48C6-8DCD-29388B8B3E40%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=10&elapsed_time=124&mr_service=1&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7B901B414B-72A2-48C6-8DCD-29388B8B3E40%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=10&elapsed_time=124&mr_service=1&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	195.362869978

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /update/2/version.txt?type=task_executed&taskid=%7B84DC8324-C256-4EF5-B0DC-383B43EE77E9%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=1875&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7B84DC8324-C256-4EF5-B0DC-383B43EE77E9%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=1875&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	195.537896872
Path: /update/2/version.txt?type=spnative_run&id=mrupdater&event=done&exit_code=0&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=317&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=spnative_run&id=mrupdater&event=done&exit_code=0&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=317&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	195.983158827
Path: /update/2/version.txt?type=task_executed&taskid=%7BB202C093-6D9F-43F2-8B6C-44FC1583EFAF%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=2466&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7BB202C093-6D9F-43F2-8B6C-44FC1583EFAF%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=2466&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	209.886955023
Path: /update/2/version.txt?type=task_executed&taskid=%7BFC604959-8A01-4E8B-A3E5-87CEEBD6FEDB%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=3057&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7BFC604959-8A01-4E8B-A3E5-87CEEBD6FEDB%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=3057&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	216.032524824
Path: /update/2/version.txt?type=prog_set&target=ch&prog=xtn_dse&event=done&mr_ext=gbnhehnpnbiioheicppmmmjaekcdfigc&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=361&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=prog_set&target=ch&prog=xtn_dse&event=done&mr_ext=gbnhehnpnbiioheicppmmmjaekcdfigc&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=361&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	300.056183815

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /update/2/version.txt?type=prog_set&target=ch&prog=xtn_hp&event=done&mr_ext=fppjhfcgnalgfiimdflmikpifodndljf&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=496&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=prog_set&target=ch&prog=xtn_hp&event=done&mr_ext=fppjhfcgnalgfiimdflmikpifodndljf&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=496&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	350.027285814
Path: /update/2/version.txt?type=task_executed&taskid=%7B2AB1F4AB-E3FA-4047-9033-EC223C8354F5%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=11583&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater **URI:** http://mrds.mail.ru/update/2/version.txt?type=task_executed&taskid=%7B2AB1F4AB-E3FA-4047-9033-EC223C8354F5%7D&done=1&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.176&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=12&elapsed_time=11583&mr_service=0&os=win6.1&install_id=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&GUID=%7BFDDD13D1-C518-46F4-AF38-584C93AD065A%7D&tool=mrupdater						
mrds.mail.ru	80	GET	1.1	AmigoLoader	1	360.045928001
Path: /update/2/version.txt?GUID={BE6997F4-D488-4E58-BAAF-8DB21A213BEE}&os=6.1&type=mloader_downloaded&newrfr=mediaplay **URI:** http://mrds.mail.ru/update/2/version.txt?GUID={BE6997F4-D488-4E58-BAAF-8DB21A213BEE}&os=6.1&type=mloader_downloaded&newrfr=mediaplay						
mrds.mail.ru	80	GET	1.1	MRDA/1	1	385.255182028
Path: /update/2/version.txt?type=prog_set&target=ch&prog=xtn_pult&event=done&mr_ext=ebkgajjadgojjkgacfgjpnpgagpecpjp&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=594&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules= **URI:** http://mrds.mail.ru/update/2/version.txt?type=prog_set&target=ch&prog=xtn_pult&event=done&mr_ext=ebkgajjadgojjkgacfgjpnpgagpecpjp&masterid=%7B6F701F8A-827D-4022-B9D7-591EA0276DB0%7D&user_id=%7BC3B64E02-D00F-40E8-955A-2712768AF7BF%7D&osver=7&osbit=64&osvernum=6.1&ossp=Service%20Pack%201&uac=0&admin=1&ver=5.0.0.172&mailru_guard=0&mailru_updater=1&comp_mem=3071&tool_mem=19&elapsed_time=594&mr_service=0&os=win6.1&tool=sputnik&GUID=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&common_rfr=&install_id=%7B7A3443F0-1262-404C-9669-83BD646EA222%7D&rfr_rules=						

DNS QUERIES

Request	Type
download.mediaplay.ru	A
Answers - mediaplay.ru (CNAME) - 193.0.201.76 (A)	
amigobin.cdnmail.ru	A
Answers - 94.100.180.110 (A) - moscow.cdnmail.ru (CNAME)	
sputnikmailru.cdnmail.ru	A
Answers - 217.69.139.110 (A)	
xmlbinupdate.mail.ru	A

Request	Type
Answers - 217.69.139.247 (A)	
conserv.go.mail.ru	A
Answers - 217.69.139.122 (A)	
mrds.mail.ru	A
Answers - 217.69.139.245 (A)	
goappsdl.distribmail.ru	A
Answers - goappsdl.cdnmail.ru (CNAME)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.215.131.194 (A) - a1621.g.akamai.net (CNAME) - 23.215.131.177 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.digicert.com	A
Answers - 93.184.220.29 (A) - cs9.wac.phicdn.net (CNAME)	
status.geotrust.com	A
Answers - ocsp.digicert.com (CNAME) - 72.21.91.29 (A)	
crl.microsoft.com	A
Answers - crl.www.ms.akadns.net (CNAME) - 23.215.131.200 (A) - 23.215.131.195 (A) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 151.101.66.133 (A) - 151.101.2.133 (A) - global.prd.cdn.globalsign.com (CNAME) - 151.101.194.133 (A) - 151.101.130.133 (A) - prod.globalsign.map.fastly.net (CNAME)	
install.mediaplay.ru	A
mailruupdater.cdnmail.ru	A
xtnmailru.cdnmail.ru	A
gosoftdl.mail.ru	A

Request	Type
Answers - gosoftdl.cdnmail.ru (CNAME)	
binupdate.mail.ru	A

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
16.456859827	Sandbox	193.0.201.76	80
17.2857789993	Sandbox	94.100.180.110	80
18.4224359989	Sandbox	217.69.139.110	80
18.7048649788	Sandbox	193.0.201.76	80
86.6489720345	Sandbox	217.69.139.110	80
91.2654488087	Sandbox	217.69.139.110	80
111.815402031	Sandbox	217.69.139.247	443
113.356535912	Sandbox	217.69.139.122	443
114.284623861	Sandbox	217.69.139.245	443
115.154958963	Sandbox	217.69.139.245	80
115.381068945	Sandbox	217.69.139.245	80
115.775806904	Sandbox	217.69.139.245	80
116.56900692	Sandbox	94.100.180.110	443
117.681352854	Sandbox	23.215.131.177	80
118.372571945	Sandbox	93.184.220.29	80
118.732784986	Sandbox	72.21.91.29	80
119.712499857	Sandbox	94.100.180.110	443
120.346436977	Sandbox	94.100.180.110	443
164.301146984	Sandbox	23.215.131.200	80
164.672330856	Sandbox	151.101.2.133	80
166.389979839	Sandbox	193.0.201.76	443
167.701465845	Sandbox	23.215.131.194	80
175.73230195	Sandbox	217.69.139.245	80
176.344358921	Sandbox	217.69.139.245	80
176.740592003	Sandbox	94.100.180.110	443
176.917671919	Sandbox	94.100.180.110	443
176.93561697	Sandbox	217.69.139.245	80
177.457403898	Sandbox	217.69.139.245	80
177.708417892	Sandbox	94.100.180.110	443
177.979858875	Sandbox	217.69.139.245	80
178.732656956	Sandbox	94.100.180.110	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
181.836745977	Sandbox	94.100.180.110	443
181.860880852	Sandbox	217.69.139.245	80
183.036386967	Sandbox	94.100.180.110	443
184.287325859	Sandbox	217.69.139.245	80
184.350324869	Sandbox	94.100.180.110	443
188.09518981	Sandbox	94.100.180.110	443
190.411587	Sandbox	94.100.180.110	443
190.596354961	Sandbox	217.69.139.245	80
190.614584923	Sandbox	217.69.139.245	443
190.712621927	Sandbox	217.69.139.247	443
190.716437817	Sandbox	217.69.139.247	443
192.216838837	Sandbox	217.69.139.245	80
193.085071802	Sandbox	217.69.139.245	80
193.212225914	Sandbox	217.69.139.245	80
193.560796022	Sandbox	217.69.139.245	80
193.574321985	Sandbox	217.69.139.245	80
193.716240883	Sandbox	217.69.139.245	80
193.728782892	Sandbox	217.69.139.245	443
193.852687836	Sandbox	217.69.139.247	443
194.296264887	Sandbox	217.69.139.245	80
194.846709013	Sandbox	217.69.139.245	80
194.872252941	Sandbox	217.69.139.245	80
195.362869978	Sandbox	217.69.139.245	80
195.537896872	Sandbox	217.69.139.245	80
195.983158827	Sandbox	217.69.139.245	80
209.886955023	Sandbox	217.69.139.245	80
216.032524824	Sandbox	217.69.139.245	80
300.056183815	Sandbox	217.69.139.245	80
350.027285814	Sandbox	217.69.139.245	80
360.045928001	Sandbox	217.69.139.245	80
385.255182028	Sandbox	217.69.139.245	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.24413895607	Sandbox	192.168.56.255	137
7.28672385216	Sandbox	224.0.0.252	5355
7.30631399155	Sandbox	224.0.0.252	5355
7.31304788589	Sandbox	239.255.255.250	3702
9.86669898033	Sandbox	224.0.0.252	5355
13.3217799664	Sandbox	192.168.56.255	138
16.0991380215	Sandbox	8.8.4.4	53
16.6236159801	Sandbox	8.8.4.4	53
17.5045588017	Sandbox	8.8.4.4	53
85.8525028229	Sandbox	8.8.4.4	53
90.3958280087	Sandbox	8.8.4.4	53
111.414191008	Sandbox	8.8.4.4	53
112.15918684	Sandbox	224.0.0.252	5355
113.058279991	Sandbox	8.8.4.4	53
114.056185007	Sandbox	8.8.4.4	53
116.098493814	Sandbox	8.8.4.4	53
117.619067907	Sandbox	8.8.4.4	53
118.270742893	Sandbox	8.8.4.4	53
118.687569857	Sandbox	8.8.4.4	53
164.228793859	Sandbox	8.8.4.4	53
164.622646809	Sandbox	8.8.4.4	53
166.111091852	Sandbox	8.8.4.4	53
167.587906837	Sandbox	8.8.4.4	53
175.943212986	Sandbox	8.8.4.4	53
176.093348026	Sandbox	8.8.4.4	53
189.962358952	Sandbox	8.8.4.4	53
190.300376892	Sandbox	8.8.4.4	53
190.461405993	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp\Microsoft.VC90.CRT.Manifest	**Type :** XML document text **MD5 :** 6bb5d2aad0ae1b4a82e7ddf7cf58802a **SHA-1 :** 70f7482f5f5c89ce09e26d745c532a9415cd5313 **SHA-256 :** 9e0220511d4ebdb014cc17ecb8319d57e3b0fea(**SHA-512 :** 3ea373dacfd3816405f6268ac05886a7dc870975: **Size :** 0.524 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp\Msvcp90.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4c39358ebdd2ffcd9132a30e1ec31e16 **SHA-1 :** 70ac82988285f9f7069faa9a0612aeba7fb001c4 **SHA-256 :** 06918cf99ad26cd6cf106881c0d5bdb212dc0bac **SHA-512 :** eb5348d2f258767281fe954d45999bd6eb7af614 **Size :** 569.68 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cookies.Sqlite-Shm	**Type :** FoxPro FPT, blocks size 0, next free block index 417475840 **MD5 :** b7c14ec6110fa820ca6b65f5aec85911 **SHA-1 :** 608eeb7488042453c9ca40f7e1398fc1a270f3f4 **SHA-256 :** fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e **SHA-512 :** d8d75760f29b1e27ac9430bc4f4ffcec39f1590be5 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Temp\Tar8C79.Tmp	**Type :** data **MD5 :** 64902cc52cf1cc2739c564325b8dd55a **SHA-1 :** d6d8ea05343c5629b7446f6b3f036d8cce168fd5 **SHA-256 :** d97a11d07b0491776def454680d2db5e5d0252b **SHA-512 :** dc552f81847fedc7db48c76510975eaccf8ab8fd3 **Size :** 130.662 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp\Msvcm90.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** d34a527493f39af4491b3e909dc697ca **SHA-1 :** afee32fcd9ce160680371357a072f58c5f790d48 **SHA-256 :** 7a74da389fbd10a710c294c2e914dc6f18e05f028 **SHA-512 :** 0dabc5455eb02601d7c40a9c49b3ade750b1118 **Size :** 225.28 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp_isetup_shfoldr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 92dc6ef532fbb4a5c3201469a5b5eb63 **SHA-1 :** 3e89ff837147c16b4e41c30d6c796374e0b8e62c **SHA-256 :** 9884e9d1b4f8a873ccbd81f8ad0ae257776d2348 **SHA-512 :** 9908e573921d5dbc3454a1c0a6c969ab8a81cc2e **Size :** 23.312 Kilobytes.
C:\Users\User\AppData\Local\Temp\3167-B30a-014e-E4c0\Fppjhfcgnalgfiimdflmikpifodndljf\Manifest.Json	**Type :** UTF-8 Unicode text, with very long lines, with CRLF line terminators **MD5 :** a457b472723f89c07f6aa361b1674bf0 **SHA-1 :** a8714311803dfef9ad9e8982a52ca06442e67a96 **SHA-256 :** ed35790bff44d1b4cfb4f2f4f8b9d744389eefc920 **SHA-512 :** ca52ce04cc4b0232607790f9d50ebbce9ef40b56f **Size :** 1.28 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Dc3e-9e83-Da0d-A1c8\Gbnhehnpnbiioheicppmmmjaekcdfigc\Manifest.Json	**Type :** UTF-8 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 51de216945b3d5b958d7f3625ca3935a **SHA-1 :** 9ff47562860021b255f538f0757e26cdc805143f **SHA-256 :** 2c586c5c31c5f3f84dd20ac5b85f74624c64e65fd **SHA-512 :** 85f854fa7db886706029073aa9643ede4bc42543 **Size :** 1.481 Kilobytes.
C:\Users\User\AppData\Local\Temp\Cab8C78.Tmp	**Type :** Microsoft Cabinet archive data, 54153 bytes, 1 file **MD5 :** 767760b1b3b838b2de0599d0e76d1c76 **SHA-1 :** c56b126f887495918e8abcf813957780f0b9466a **SHA-256 :** c0f37380971fb93ecb0cfa3c2bd6d91cc77f254f0a **SHA-512 :** bacdd86b37e70fe36274c6ae9076f0ac89e82245 **Size :** 54.153 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-OP7S1.Tmp\4618f1ae573e668331fa830efcc1c8050c23eff1.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 55233dd9d22cfa4b0a913bd8db9c3e14 **SHA-1 :** 7bede1757326e5124fe65b4afaec5a137b25e943 **SHA-256 :** d584102f46454f9a85fc177ac8bfbbcc08efd9ce8 **SHA-512 :** 4dfa0c002766b44809152baa9724bc7b0b7c45f7 **Size :** 1499.648 Kilobytes.
C:\Users\User\AppData\Local\Temp\E45e-9fa6-6843-8bb8\Na_runner.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** feb798265c24beb577cb5bcd43cbd158 **SHA-1 :** 0b13b0b60367a77cdc55a8db5c31dd7c1f1f7162 **SHA-256 :** d9be17d76dfb9d90246512ce89dd7aab7cf1cf94 **SHA-512 :** 157024ad7e3b1ea71c6e398105506d7a3df9c875 **Size :** 3620.536 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp\Msvcr90.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** cdbe9690cf2b8409facad94fac9479c9 **SHA-1 :** 4bcdfe2c1b354645314a4ce26b55b2b1a0212db9 **SHA-256 :** 8e7fe1a1f3550c479ffd86a77bc9d10686d47f872 **SHA-512 :** 9c84ed9a66ce20a22e14fa00c1a0db716133f7b2 **Size :** 653.136 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** 4ff75f505fddcc6a9ae62216446205d9 **SHA-1 :** efe32d504ce72f32e92dcf01aa2752b04d81a342 **SHA-256 :** a4c86fc4836ac728d7bd96e7915090fd59521a9e **SHA-512 :** ba0469851438212d19906d6da8c4ae95ff1c0711 **Size :** 6.144 Kilobytes.
C:\Users\User\AppData\Local\Temp\64f2-798a-6964-0384	**Type :** 7-zip archive data, version 0.4 **MD5 :** 513d796fa94eef7669f14bef4f749a82 **SHA-1 :** ca370adff9c0b153f0b913578e5cf47dca6fa3be **SHA-256 :** a38a68c49f168d1e8baa2f68c9123405d12cdd85 **SHA-512 :** e63af7d5603620b6409f3a5ce4b13609506aee84 **Size :** 354.481 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp\Mail_logo.Bmp	**Type :** PC bitmap, Windows 3.x format, 248 x 68 x 24 **MD5 :** fa810d88b738f98cde6c3a09a256f524 **SHA-1 :** abc7351e03e96243594d868f50a20b437c2bff2a **SHA-256 :** 4deec7b28055c6c3cdcb3d76125f5cd41219508f **SHA-512 :** 83ad355259a816ee1fae46d45352cf048aeec94a **Size :** 50.646 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-47I4P.Tmp\Itdownload.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d82a429efd885ca0f324dd92afb6b7b8 **SHA-1 :** 86bbdaa15e6fc5c7779ac69c84e53c43c9eb20ea **SHA-256 :** b258c4d7d2113dee2168ed7e35568c8e03341e2 **SHA-512 :** 5bf0c3b8fa5db63205a263c4fa5337188173248b **Size :** 205.312 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	MediaPlay_id3754771id.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	4618f1ae573e668331fa830efcc1c8050c23eff1
MD5:	786bdcc6f403a6bde9ef002e19e391ac
First Seen Date:	2016-07-23 19:37:11.880366 (3 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2016-07-23 19:37:11.880366 (3 years ago)
Human Expert Analysis Date:	2019-01-16 05:46:56.267639 (about a month ago)
Human Expert Analysis Result:	Clean

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	8
Compilation Time Stamp	0x4EF6EA4C [Sun Dec 25 09:18:04 2011 UTC]
LegalCopyright	
FileVersion	
CompanyName	MediaPlay LLC
Comments	This installation was built with Inno Setup.
ProductName	MediaPlay
ProductVersion	1.0
FileDescription	MediaPlay Setup
Translation	0x0000 0x04b0
Entry Point	0x416478 (.itext)
Machine Type	Intel 386 or later - 32Bit
File Size	1786320
Sha256	d5595fc9c25a9ad2be2c1a0450c0b7f6f978da2deaabf03fdd0e3b544da56ba8
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x143f0	0x14400	6.482184	-
.itext	0x16000	0xbe8	0xc00	6.009848	-
.data	0x17000	0xd9c	0xe00	2.674099	-
.bss	0x18000	0x5714	0x0	0.000000[SUSPICIOUS]	-
.idata	0x1e000	0xf9e	0x1000	4.967783	-
.tls	0x1f000	0x8	0x0	0.000000[SUSPICIOUS]	-
.rdata	0x20000	0x18	0x200	0.190489[SUSPICIOUS]	-
.rsrc	0x21000	0xe408	0xe600	5.271044	-

PE Imports

- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
  - SysAllocStringLen
- advapi32.dll
  - RegQueryValueExW
  - RegOpenKeyExW

    - RegCloseKey
- user32.dll
    - GetKeyboardType
    - LoadStringW
    - MessageBoxA
    - CharNextW
- kernel32.dll
    - GetACP
    - Sleep
    - VirtualFree
    - VirtualAlloc
    - GetSystemInfo
    - GetTickCount
    - QueryPerformanceCounter
    - GetVersion
    - GetCurrentThreadId
    - VirtualQuery
    - WideCharToMultiByte
    - MultiByteToWideChar
    - lstrlenW
    - lstrcpynW
    - LoadLibraryExW
    - GetThreadLocale
    - GetStartupInfoA
    - GetProcAddress
    - GetModuleHandleW
    - GetModuleFileNameW
    - GetLocaleInfoW
    - GetCommandLineW
    - FreeLibrary
    - FindFirstFileW
    - FindClose
    - ExitProcess
    - WriteFile
    - UnhandledExceptionFilter
    - RtlUnwind
    - RaiseException
    - GetStdHandle
    - CloseHandle
- kernel32.dll
    - TlsSetValue
    - TlsGetValue
    - LocalAlloc
    - GetModuleHandleW
- user32.dll
    - CreateWindowExW
    - TranslateMessage
    - SetWindowLongW
    - PeekMessageW
    - MsgWaitForMultipleObjects
    - MessageBoxW
    - LoadStringW
    - GetSystemMetrics
    - ExitWindowsEx
    - DispatchMessageW
    - DestroyWindow
    - CharUpperBuffW
    - CallWindowProcW
- kernel32.dll
    - WriteFile
    - WideCharToMultiByte
    - WaitForSingleObject
    - VirtualQuery
    - VirtualProtect
    - VirtualFree
    - VirtualAlloc
    - SizeofResource
    - SignalObjectAndWait
    - SetLastError
    - SetFilePointer
    - SetEvent
    - SetErrorMode
    - SetEndOfFile
    - ResetEvent
    - RemoveDirectoryW

    - ReadFile
    - MultiByteToWideChar
    - LockResource
    - LoadResource
    - LoadLibraryW
    - LeaveCriticalSection
    - InitializeCriticalSection
    - GetWindowsDirectoryW
    - GetVersionExW
    - GetUserDefaultLangID
    - GetThreadLocale
    - GetSystemInfo
    - GetStdHandle
    - GetProcAddress
    - GetModuleHandleW
    - GetModuleFileNameW
    - GetLocaleInfoW
    - GetLocalTime
    - GetLastError
    - GetFullPathNameW
    - GetFileSize
    - GetFileAttributesW
    - GetExitCodeProcess
    - GetEnvironmentVariableW
    - GetDiskFreeSpaceW
    - GetDateFormatW
    - GetCurrentProcess
    - GetCommandLineW
    - GetCPInfo
    - InterlockedExchange
    - InterlockedCompareExchange
    - FreeLibrary
    - FormatMessageW
    - FindResourceW
    - EnumCalendarInfoW
    - EnterCriticalSection
    - DeleteFileW
    - DeleteCriticalSection
    - CreateProcessW
    - CreateFileW
    - CreateEventW
    - CreateDirectoryW
    - CompareStringW
    - CloseHandle
- advapi32.dll
    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
    - OpenProcessToken
    - LookupPrivilegeValueW
- comctl32.dll
    - InitCommonControls
- kernel32.dll
    - Sleep
- advapi32.dll
    - AdjustTokenPrivileges
- oleaut32.dll
    - SafeArrayPtrOfIndex
    - SafeArrayGetUBound
    - SafeArrayGetLBound
    - SafeArrayCreate
    - VariantChangeType
    - VariantCopy
    - VariantClear
    - VariantInit

PE Resources

RT_ICON
RT_STRING
RT_RCDATA
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

- Success ✔

[+] Media, LLC	
Status	NotTimeValid (no effect on chain status)
Start Date	2013-05-16 00:00:00+00:00
End Date	2016-05-15 23:59:59+00:00
Sha256	6313f94f797cf7b3bbe3c8b19dc3ae44ee604b5363990b3dc000bf027a0572dd
Serial	00888D89600E3B2E7392B928DD5903A546
Subject Key Identifier	31 6f df c5 19 a2 44 3e 7b 0b 2e 0a 30 00 66 05 c1 c8 84 9a
Issuer Name	COMODO Code Signing CA 2
Issuer Key Identifier	1e c5 b1 2c 7d 87 da 02 68 7c 25 bc 0c 07 84 3f b6 cf de f1
Crl link	http://crl.comodoca.com/COMODOCodeSigningCA2.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

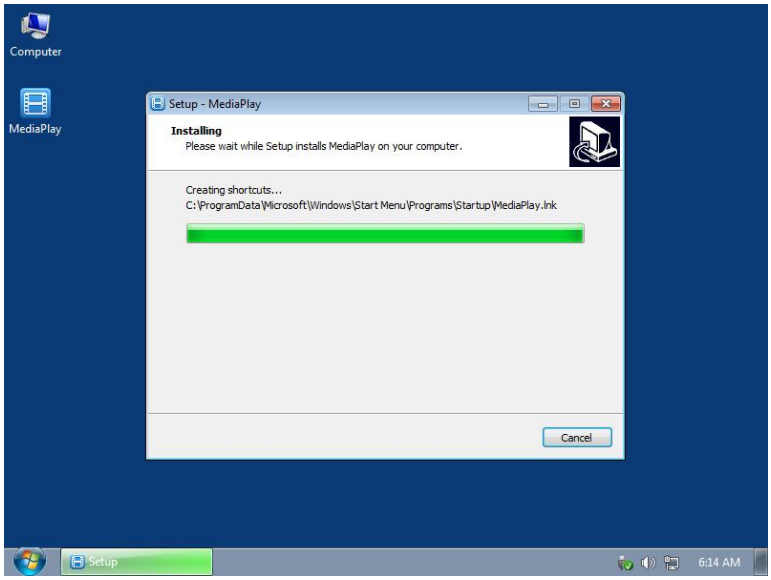
[+] COMODO Code Signing CA 2	
Status	NoError ✔
Start Date	2011-08-24 00:00:00+00:00
End Date	2020-05-30 10:48:38+00:00
Sha256	13f8e83884109001dcbe7de691b16991138b1a9337222cf9ce274ce2157533e0
Serial	10709D4FF55408D7306001D8EA9175BB
Subject Key Identifier	1e c5 b1 2c 7d 87 da 02 68 7c 25 bc 0c 07 84 3f b6 cf de f1
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

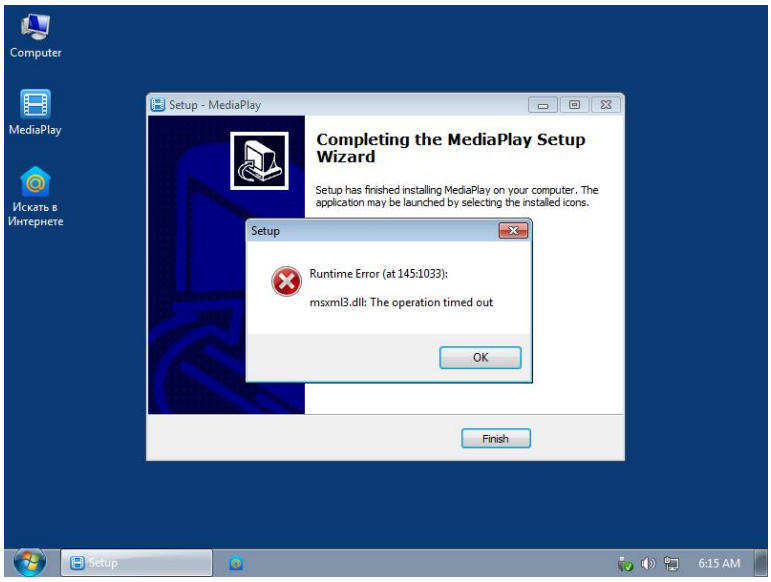
[+] UTN-USERFirst-Object	
Status	NoError ✔
Start Date	1999-07-09 18:31:20+00:00
End Date	2019-07-09 18:40:36+00:00
Sha256	2acd612cf8f03b495f01de23e4f5d695350d00ff6d27f0255362c79df0eca403
Serial	44BE0C8B500024B411D3362DE0B35F1B
Subject Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b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

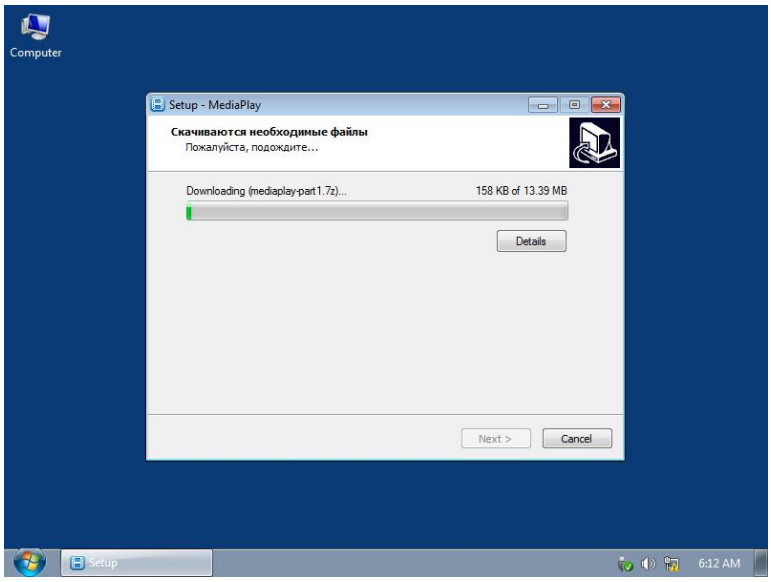
[+] COMODO Time Stamping Signer	
Status	NotTimeValid (no effect on chain status)
Start Date	2010-05-10 00:00:00+00:00
End Date	2015-05-10 23:59:59+00:00
Sha256	bc44ed62823d354042d7f98ea7679d6b54924534ee06a9c7e6ec760ae488374f
Serial	478A8EFB59E1D83F0CE142D2A28707BE
Subject Key Identifier	2e 2d b0 0a 44 4a d3 87 c0 02 07 ce 97 7d 50 62 20 fd 0f 83
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	Digital Signature,Non-Repudiation (c0)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

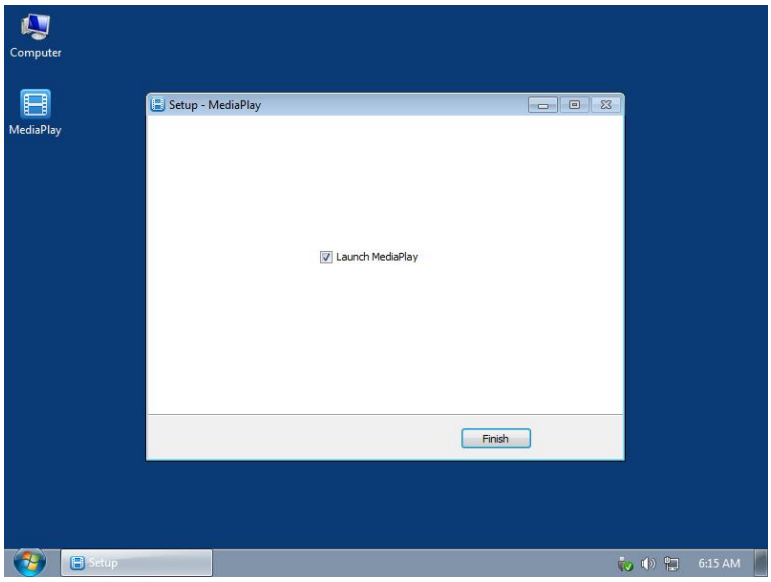
[+] UTN-USERFirst-Object	
Status	NoError ✔
Start Date	1999-07-09 18:31:20+00:00
End Date	2019-07-09 18:40:36+00:00
Sha256	2acd612cf8f03b495f01de23e4f5d695350d00ff6d27f0255362c79df0eca403
Serial	44BE0C8B500024B411D3362DE0B35F1B
Subject Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b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

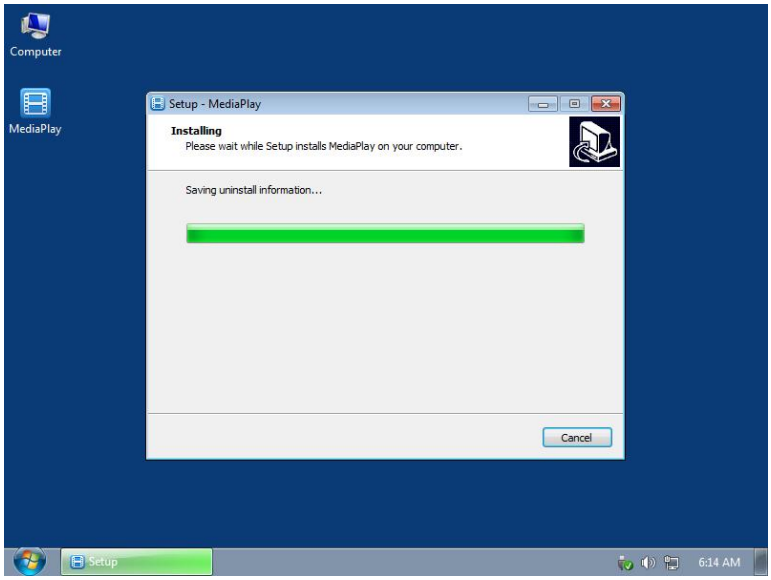
SCREENSHOTS

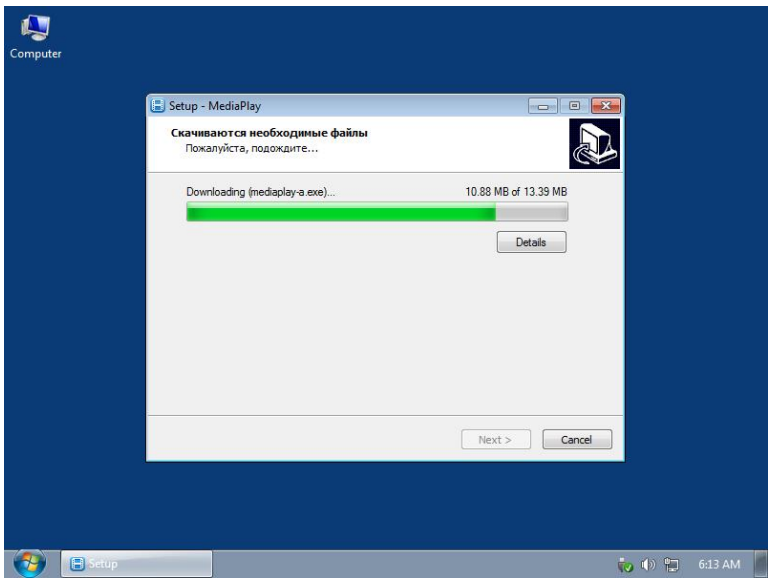


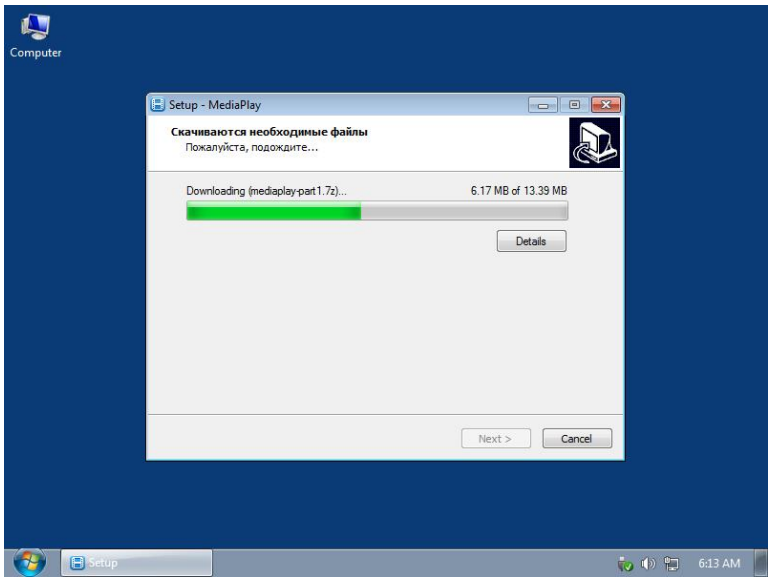


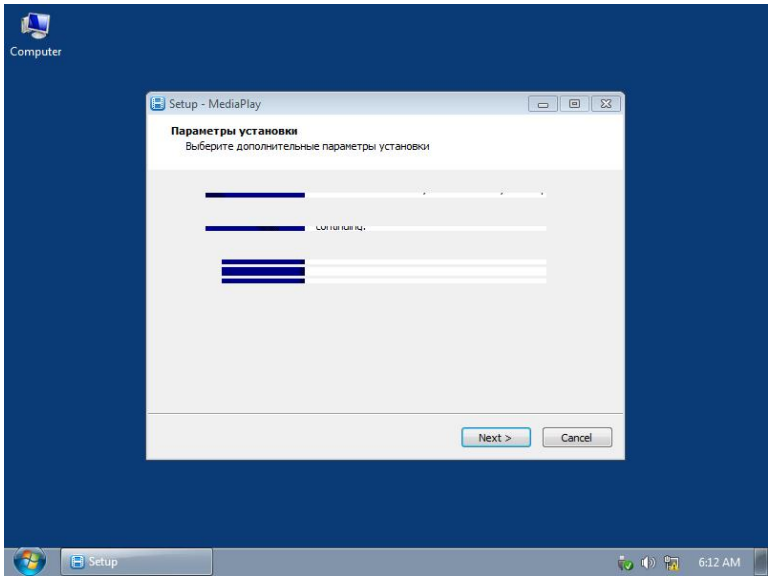


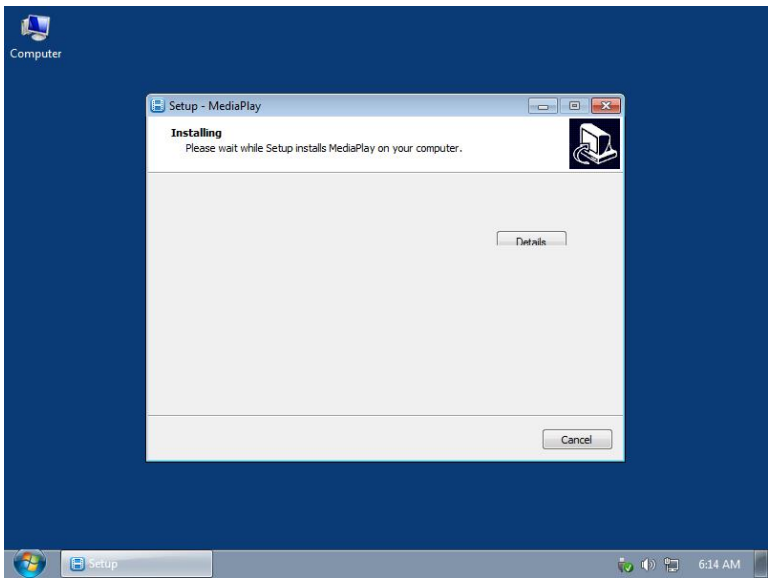

Computer
MediaPlay
Setup - MediaPlay
Launch MediaPlay
Finish
Setup
6:15 AM

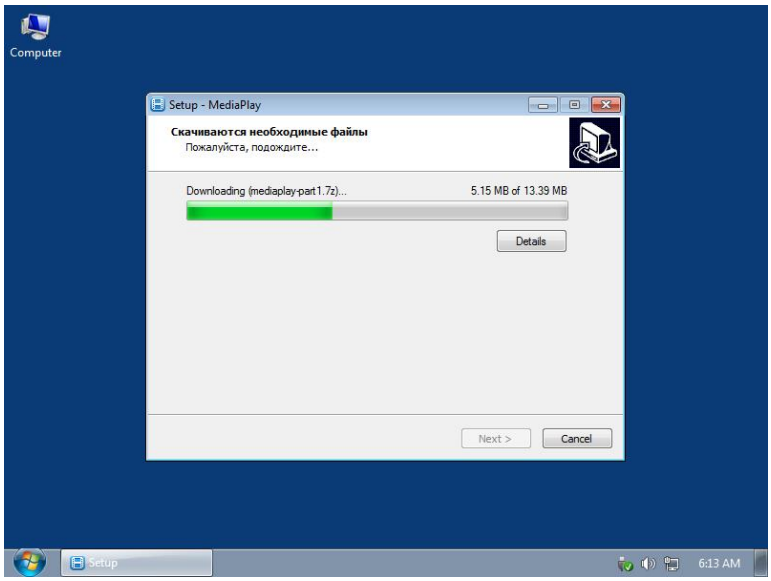

Computer
MediaPlay
Setup - MediaPlay
Installing
Please wait while Setup installs MediaPlay on your computer.
Saving uninstall information...
Cancel
Setup
6:14 AM

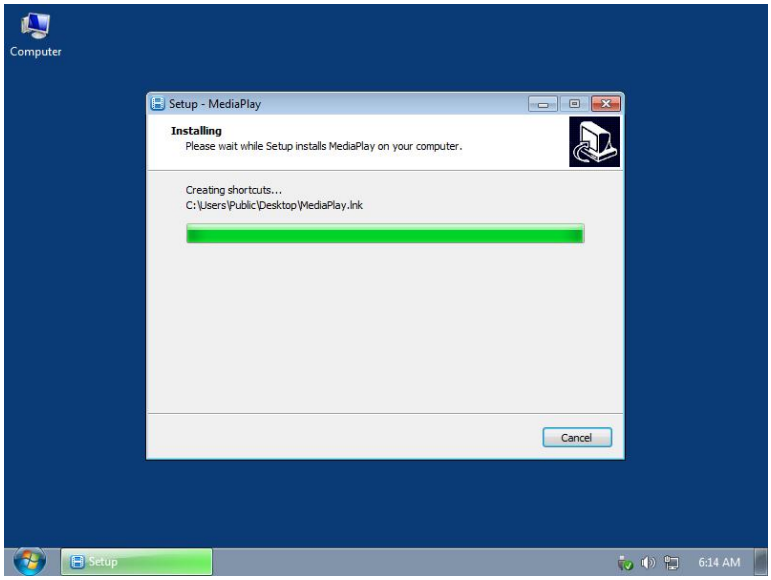

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-a.exe)...
10.88 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

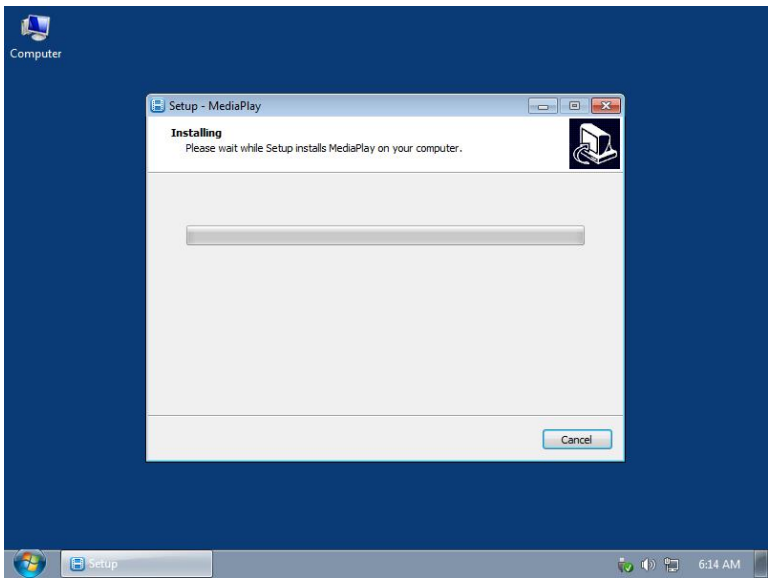

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
6.17 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

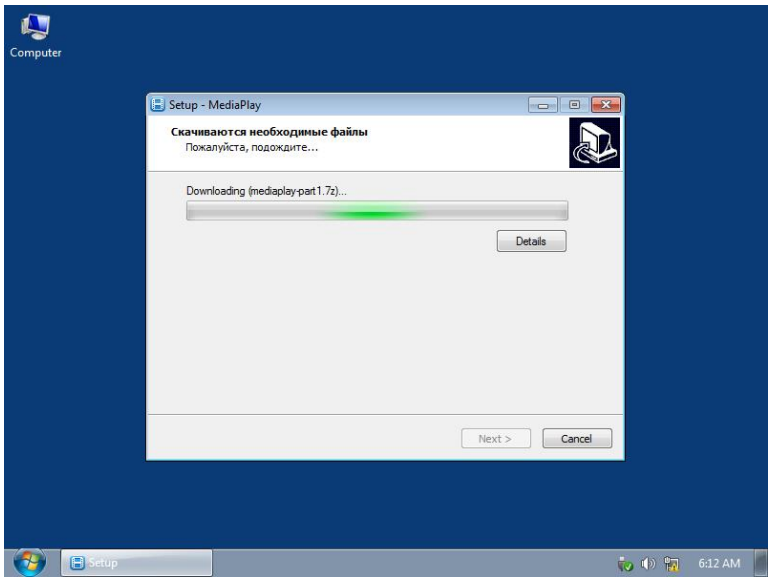

Computer
Setup - MediaPlay
Параметры установки
Выберите дополнительные параметры установки
Next >
Cancel
Setup
6:12 AM

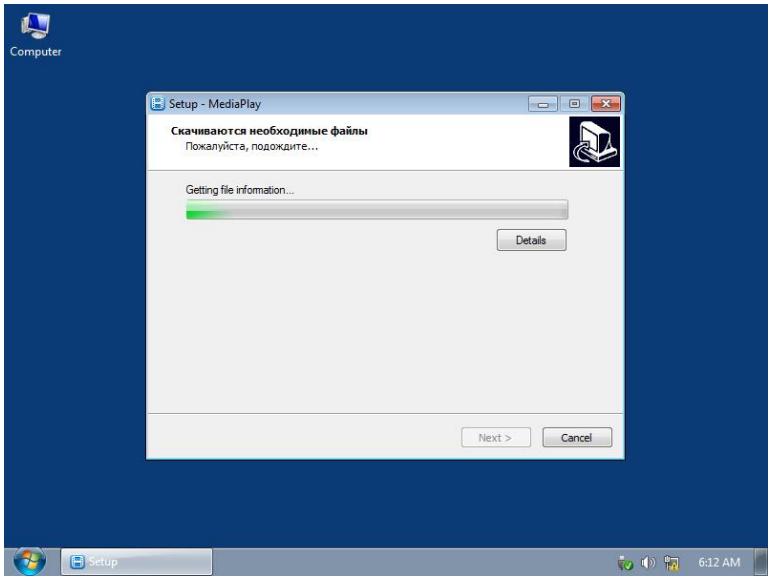

Computer
Setup - MediaPlay
Installing
Please wait while Setup installs MediaPlay on your computer.
Details
Cancel
Setup
6:14 AM

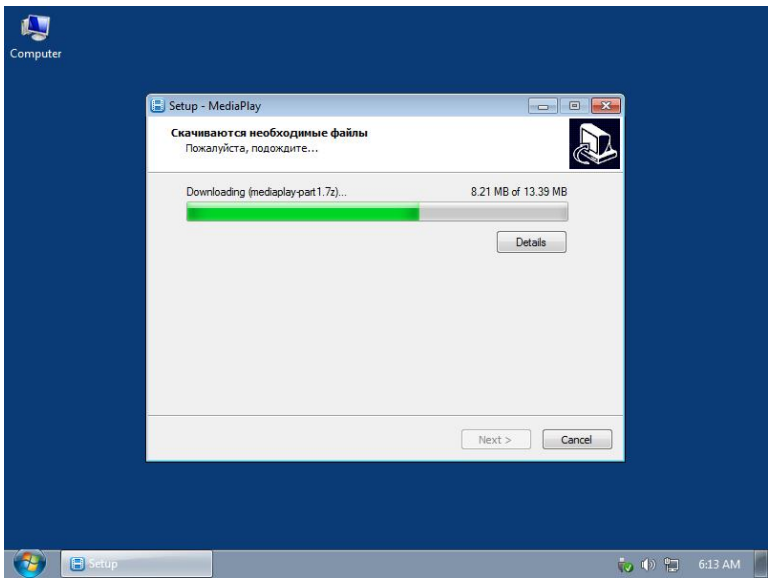

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
5.15 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

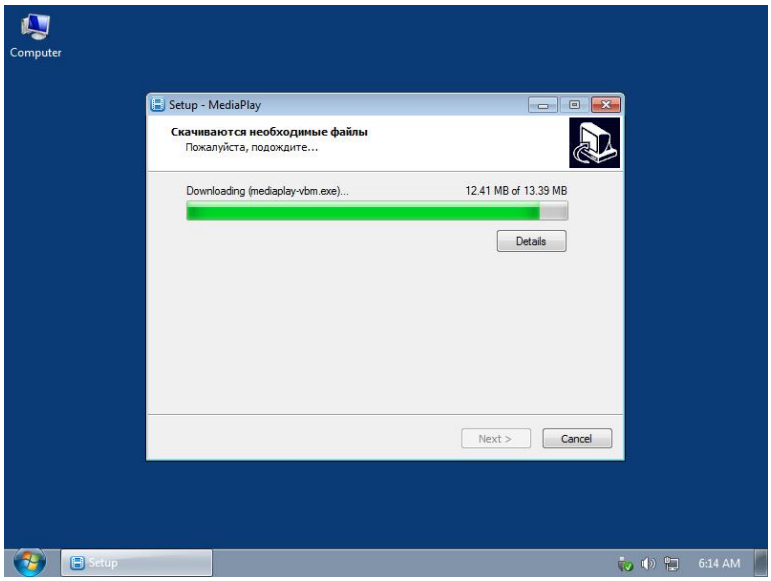

Computer
Setup - MediaPlay
Installing
Please wait while Setup installs MediaPlay on your computer.
Creating shortcuts...
C:\Users\Public\Desktop\MediaPlay.lnk
Cancel
Setup
6:14 AM

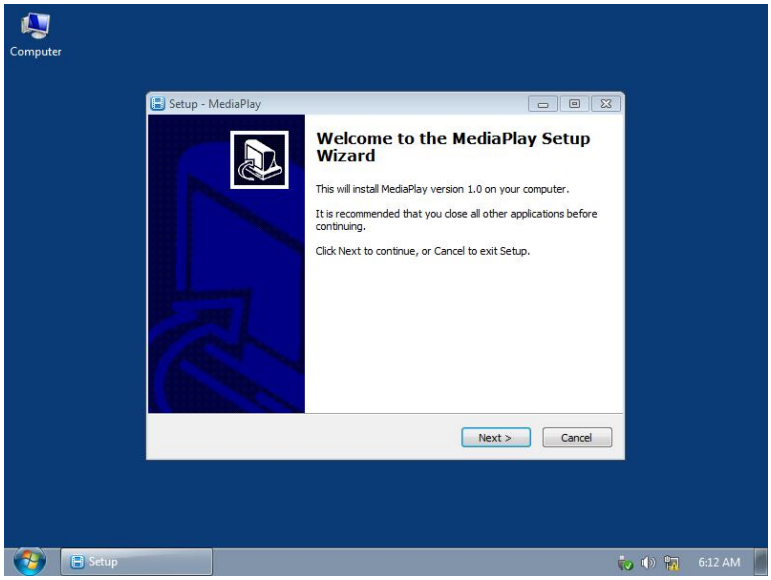

Computer
Setup - MediaPlay
Installing
Please wait while Setup installs MediaPlay on your computer.
Cancel
Setup
6:14 AM

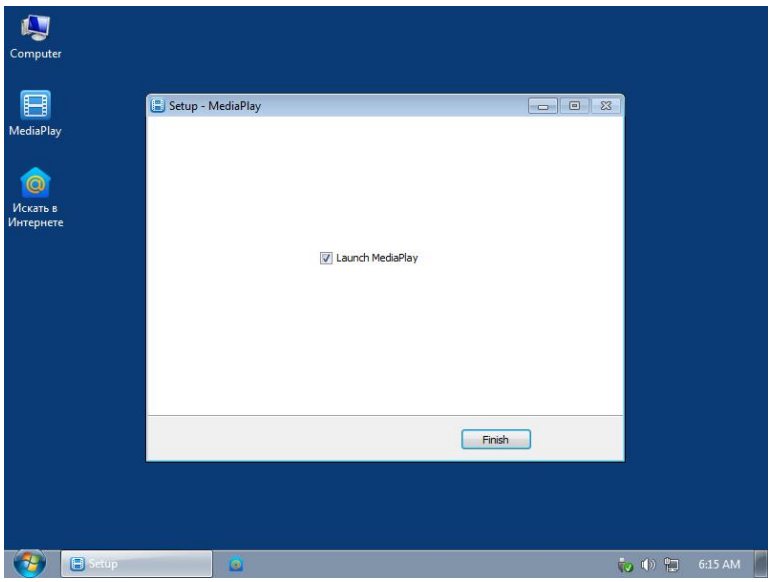

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
Details
Next >
Cancel
Setup
6:12 AM

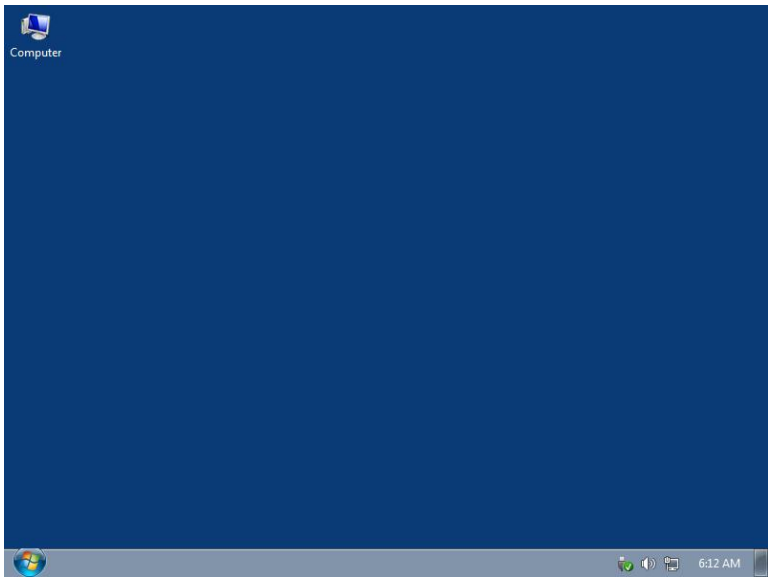

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Getting file information...
Details
Next >
Cancel
Setup
6:12 AM

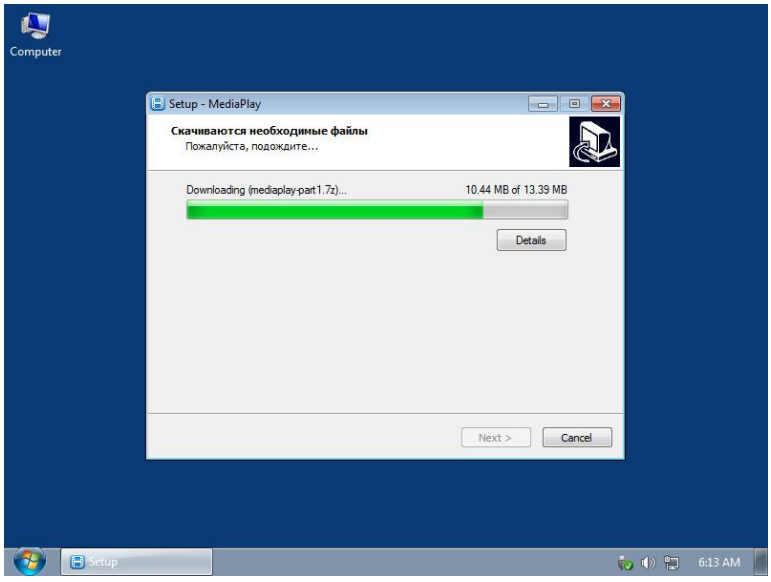

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
8.21 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

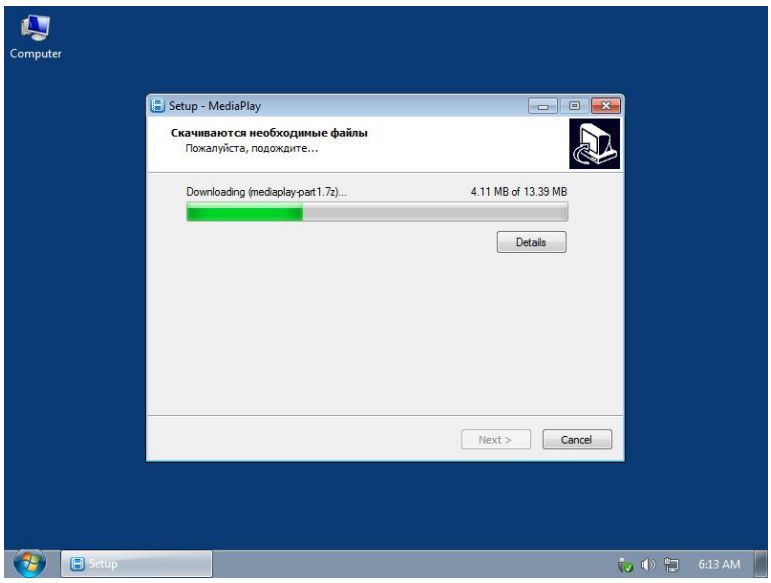

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-vbm.exe)...
12.41 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:14 AM

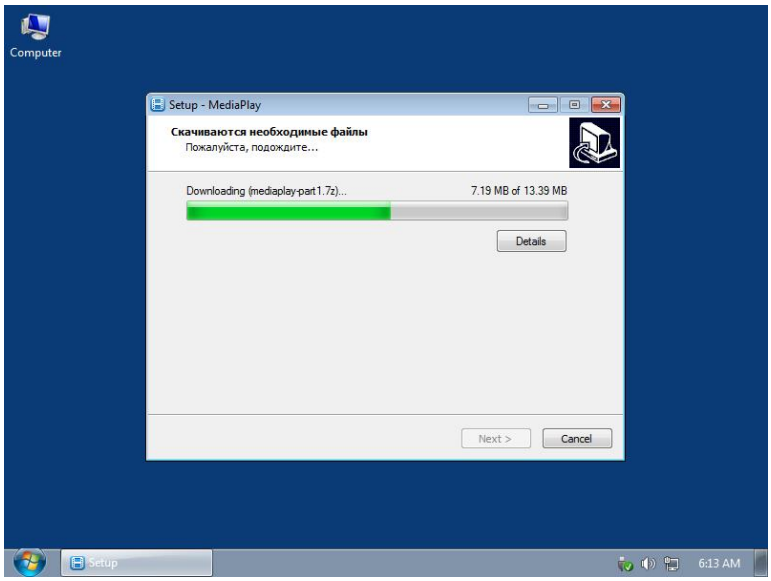

Computer
Setup - MediaPlay
Welcome to the MediaPlay Setup Wizard
This will install MediaPlay version 1.0 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
Setup
6:12 AM

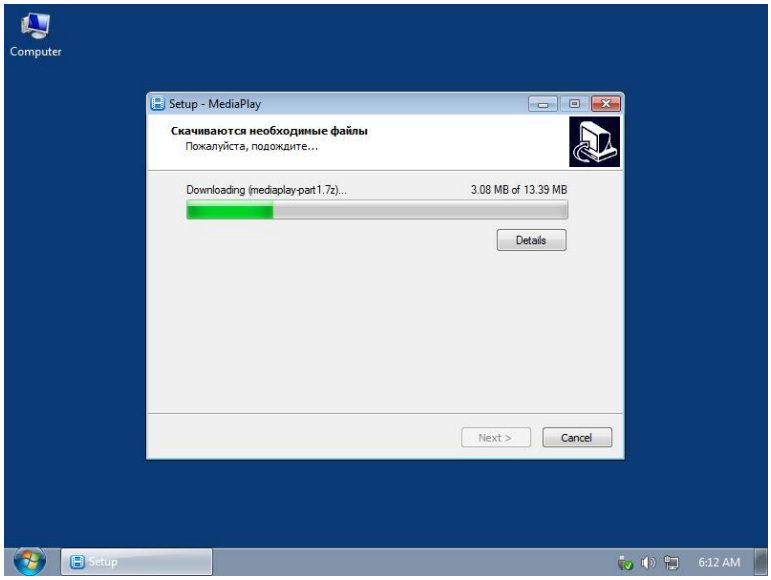

Computer
MediaPlay
Искать в Интернете
Setup - MediaPlay
Launch MediaPlay
Finish
Setup
6:15 AM

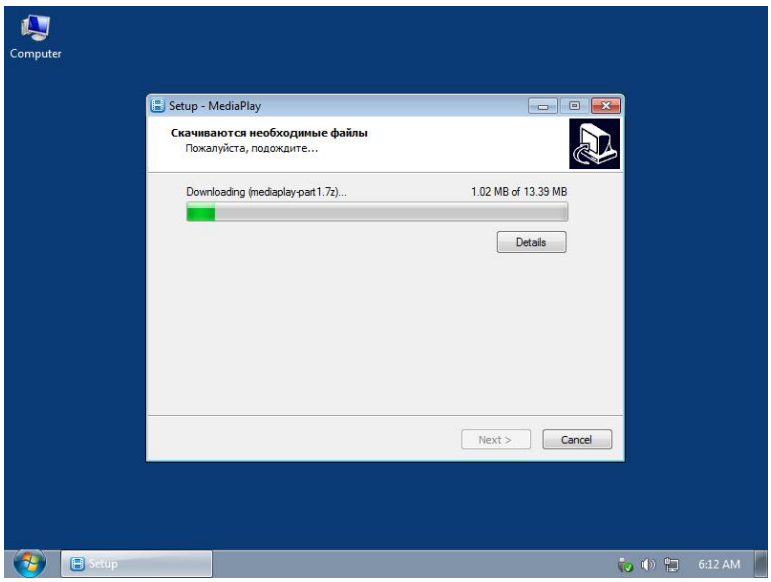

Computer
6:12 AM

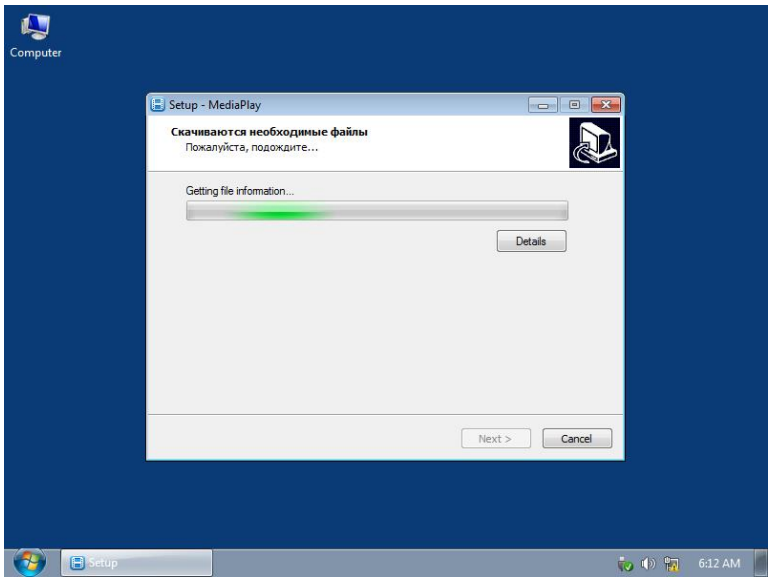

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
10.44 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

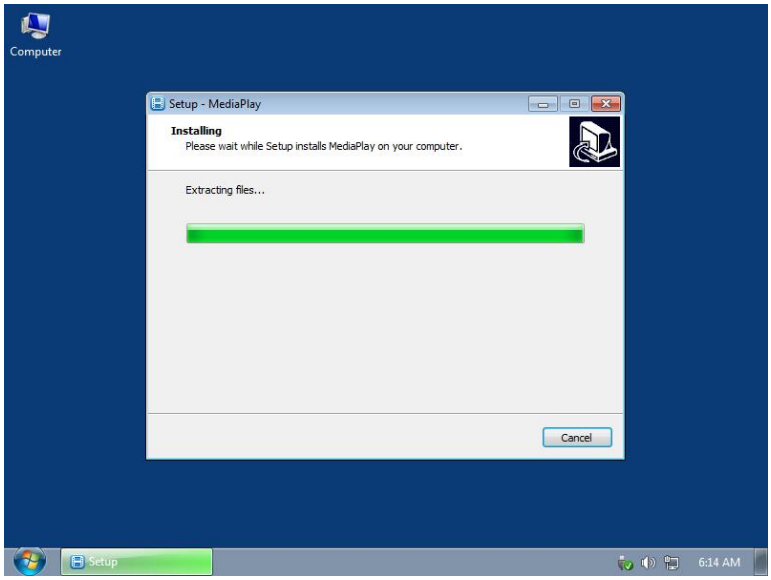

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
4.11 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

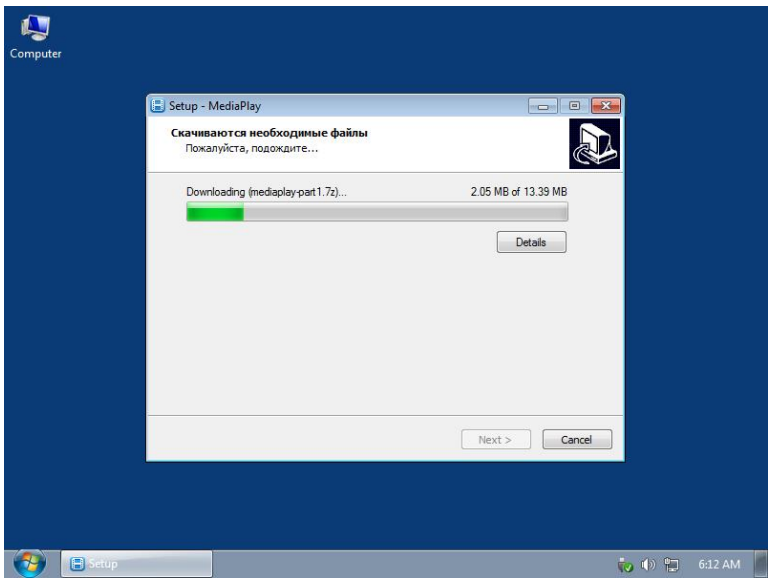

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
7.19 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM

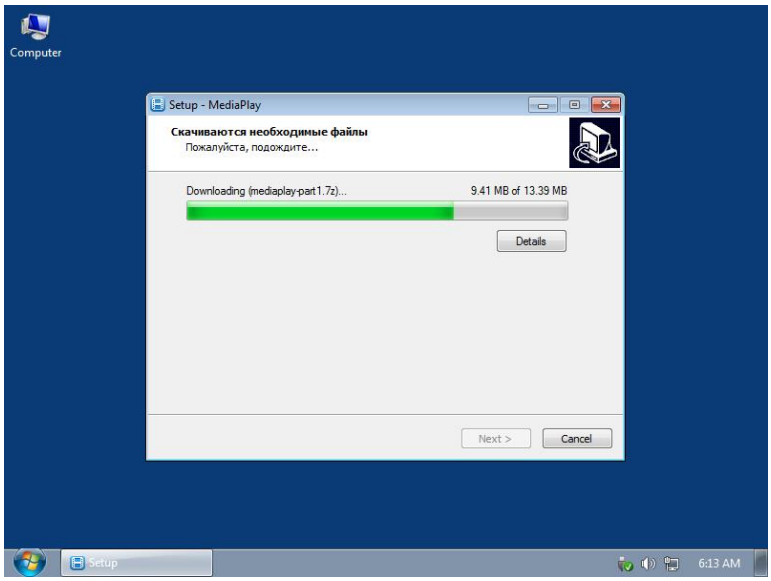

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
3.08 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:12 AM

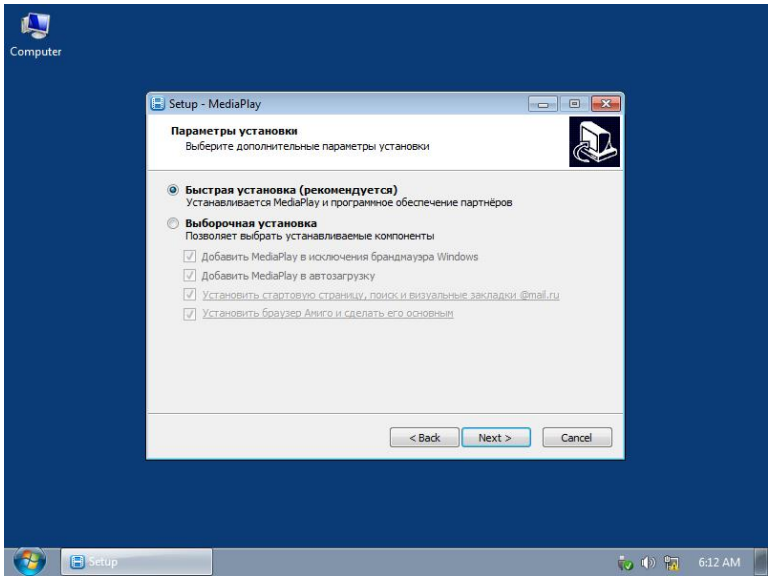

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
1.02 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:12 AM

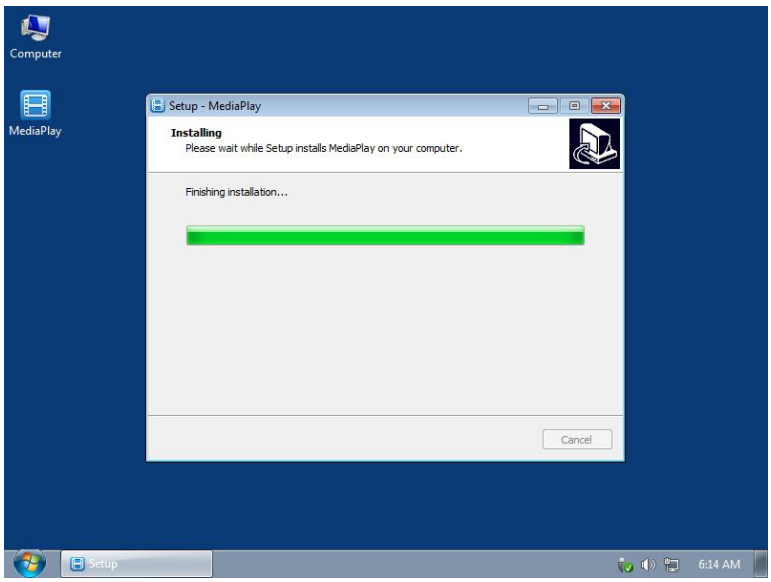

Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Getting file information...
Details
Next >
Cancel
Setup
6:12 AM

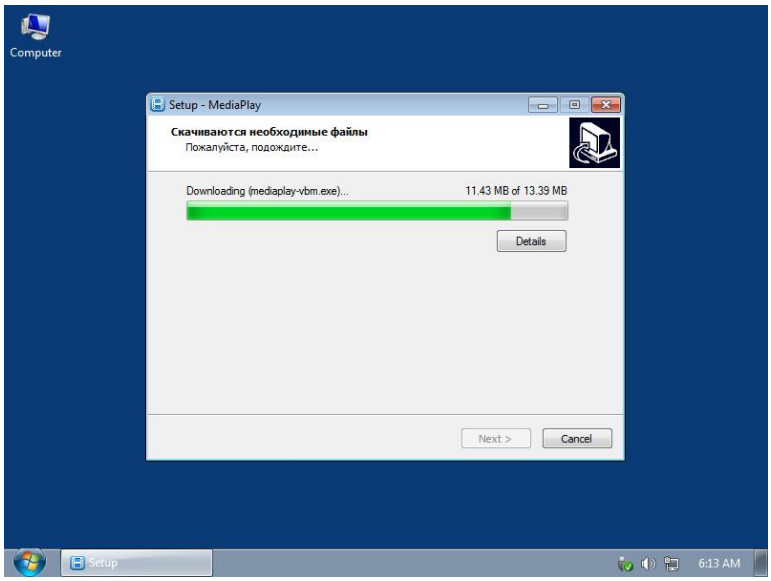

Computer
Setup - MediaPlay
Installing
Please wait while Setup installs MediaPlay on your computer.
Extracting files...
Cancel
Setup
6:14 AM


Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
2.05 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:12 AM


Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-part1.7z)...
9.41 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM


Computer
Setup - MediaPlay
Параметры установки
Выберите дополнительные параметры установки
Быстрая установка (рекомендуется)
Устанавливается MediaPlay и программное обеспечение партнёров
Выборочная установка
Позволяет выбрать устанавливаемые компоненты
Добавить MediaPlay в исключения брандмауэра Windows
Добавить MediaPlay в автозагрузку
Установить стартовую страницу, поиск и визуальные закладки @mail.ru
Установить браузер Амиго и сделать его основным
< Back
Next >
Cancel
Setup
6:12 AM


Computer
MediaPlay
Setup - MediaPlay
Installing
Please wait while Setup installs MediaPlay on your computer.
Finishing installation...
Cancel
Setup
6:14 AM


Computer
Setup - MediaPlay
Скачиваются необходимые файлы
Пожалуйста, подождите...
Downloading (mediaplay-vbm.exe)...
11.43 MB of 13.39 MB
Details
Next >
Cancel
Setup
6:13 AM