

Summary

File Name: ResMonP.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 523eb57157746d1459b46ffe5157ce084b427903
MD5: fabf007d0a26445c63be58cc1b0c5b70

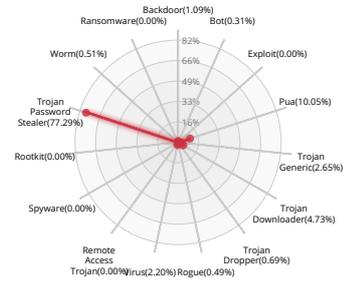


Valkyrie Final Verdict

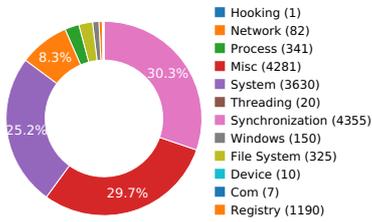
DETECTION SECTION



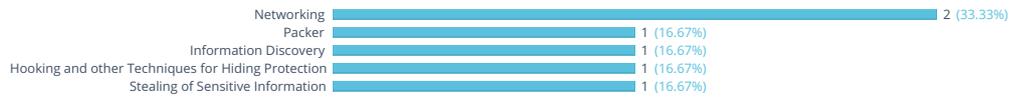
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW





Activity Details

PACKER



The binary likely contains encrypted or compressed data.

Show sources

INFORMATION DISCOVERY



Reads data out of its own binary image

Show sources

NETWORKING



Attempts to connect to a dead IP:Port (1 unique times)

Show sources

Network anomalies occurred during the analysis.

Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION



Creates RWX memory

Show sources

STEALING OF SENSITIVE INFORMATION



Harvests information related to installed mail clients

Show sources

Behavior Graph

16:00:59

16:01:24

16:01:49

PID 1932

16:00:59

Create Process

The malicious file created a child process as 523eb57157746d1459b46ffe5157ce084b427903.exe (PPID 2056)

16:00:59 NtAllocateVirtualMem

16:01:00 NtReadFile
16:01:00 [2 times]

16:01:00

Create Process

16:01:01

connect

16:01:02

getaddrinfo

16:01:31

16:01:49

connect

[2 times]

PID 2216

16:01:01

Create Process

The malicious file created a child process as splwow64.exe (PPID 1932)

Behavior Summary
ACCESSED FILES

| |
|----------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.en-US |
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.en |
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.ENU |
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.EN |
| C:\Windows\System32\tzres.dll |
| \Device\KsecDD |
| C:\Windows\Fonts\staticcache.dat |
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Users\user\AppData\Local\Temp\rbPrint.dft |
| C:\Windows\System32\rbPrint.dft |
| C:\Windows\system\rbPrint.dft |
| C:\Windows\rbPrint.dft |
| C:\ProgramData\Oracle\java\javapath\rbPrint.dft |
| C:\Windows\System32\wbem\rbPrint.dft |
| C:\Windows\System32\WindowsPowerShell\v1.0\rbPrint.dft |
| C:\Program Files\Microsoft Network Monitor 3\rbPrint.dft |
| C:\Program Files (x86)\Universal Extractor\rbPrint.dft |
| C:\Program Files (x86)\Universal Extractor\bin\rbPrint.dft |
| C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\rbPrint.dft |
| C:\Python27\rbPrint.dft |
| C:\Python27\Scripts\rbPrint.dft |
| C:\tools\sysinternals\rbPrint.dft |
| C:\tools\rbPrint.dft |
| C:\tools\IDA_Pro_v6\python\rbPrint.dft |
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.exe |
| C:\Users\user\AppData\Local\Temp\ |
| C:\Program Files (x86)\Microsoft Office\Office12\OLMAPI32.DLL |
| C:\Users\user\AppData\Local\Temp*.frc |
| C:\Windows\System32\uxtheme.dll.Config |
| C:\Windows\System32\uxtheme.dll |
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.exe.Local\ |
| C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2 |
| C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll |
| C:\Windows\WindowsShell.Manifest |
| C:\Users\user\AppData\Local\Temp\printers.xml |
| C:\Users |
| C:\Users\user |
| C:\Users\user\AppData |
| C:\Users\user\AppData\Local |
| C:\Users\user\AppData\Local\Temp |
| C:\Users\user\AppData\Local\Temp\Sejour.JNI |
| C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui |
| \\?\UNC\192.168.2.28\SQL2014\pipe\sql\query |
| C:\Program Files (x86)\Common Files\System\OLE DB\sqloledb.rll |
| C:\Program Files (x86)\Common Files\System\OLE DB\en-US\SQLOLEDB.RLL.mui |
| C:\Windows\sysnative\spool\drivers\x64\3\mxwdwui.BUD |
| C:\Windows\sysnative\spool\drivers\x64\3\mxwdwui.gpd |
| C:\Windows\sysnative\spool\drivers\x64\3\STDNAMES.GPD |
| C:\Windows\sysnative\spool\drivers\x64\3\mxwdwui.ini |
| C:\Windows\sysnative\spool\drivers\x64\3\en-US\unires.dll.mui |

C:\Windows\sysnative\spool\drivers\x64\31en-US\unidrvui.dll.mui

READ REGISTRY KEYS

| |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409 |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1 |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2 |
| 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_CURRENT_USER\Control Panel\Desktop\WindowMetrics\AppliedDPI |
| HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\DLLPathEx |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI |
| 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_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\device |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\SynchronousPrintHandleAccessMode |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\ExtensionConfig\SspiCli\CheckSignatureDll |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\ExtensionConfig\SspiCli\CheckSignatureRoutine |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SecurityProviders |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Name |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Comment |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Capabilities |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\RpcId |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Version |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Type |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\TokenSize |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Sp\WOW64TimeOut |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\SecurityService\10 |
| HKEY_CURRENT_USER\Control Panel\International\LocaleName |
| HKEY_CURRENT_USER\Control Panel\International\Country |
| HKEY_CURRENT_USER\Control Panel\International\List |
| HKEY_CURRENT_USER\Control Panel\International\Decimal |
| HKEY_CURRENT_USER\Control Panel\International\Thousand |

| |
|--------------------------------------------------------------|
| HKEY_CURRENT_USER\Control Panel\International\Grouping |
| HKEY_CURRENT_USER\Control Panel\International\NativeDigits |
| HKEY_CURRENT_USER\Control Panel\International\Currency |
| HKEY_CURRENT_USER\Control Panel\International\MonDecimalSep |
| HKEY_CURRENT_USER\Control Panel\International\MonThousandSep |
| HKEY_CURRENT_USER\Control Panel\International\MonGrouping |
| HKEY_CURRENT_USER\Control Panel\International\PositiveSign |
| HKEY_CURRENT_USER\Control Panel\International\NegativeSign |
| HKEY_CURRENT_USER\Control Panel\International\TimeFormat |
| HKEY_CURRENT_USER\Control Panel\International\ShortTime |
| HKEY_CURRENT_USER\Control Panel\International\1159 |
| HKEY_CURRENT_USER\Control Panel\International\2359 |
| HKEY_CURRENT_USER\Control Panel\International\ShortDate |
| HKEY_CURRENT_USER\Control Panel\International\YearMonth |
| HKEY_CURRENT_USER\Control Panel\International\LongDate |
| HKEY_CURRENT_USER\Control Panel\International\Country |
| HKEY_CURRENT_USER\Control Panel\International\Measure |
| HKEY_CURRENT_USER\Control Panel\International\PaperSize |
| HKEY_CURRENT_USER\Control Panel\International\Digits |
| HKEY_CURRENT_USER\Control Panel\International\Zero |
| HKEY_CURRENT_USER\Control Panel\International\NegNumber |
| HKEY_CURRENT_USER\Control Panel\International\NumShape |
| HKEY_CURRENT_USER\Control Panel\International\CurrDigits |
| HKEY_CURRENT_USER\Control Panel\International\Currency |
| HKEY_CURRENT_USER\Control Panel\International\NegCurr |
| HKEY_CURRENT_USER\Control Panel\International\CalendarType |

MODIFIED FILES

| |
|---------------------------------------------|
| C:\Users\user\AppData\Local\Temp\Sejour.INI |
| \\?\UNC\192.168.2.28\SQL2014\pipe\sql\query |

RESOLVED APIS

| |
|--------------------------------------|
| kernel32.dll.VirtualAlloc |
| kernel32.dll.VirtualFree |
| kernel32.dll.VirtualProtect |
| oleaut32.dll.SysFreeString |
| oleaut32.dll.SysReAllocStringLen |
| oleaut32.dll.SysAllocStringLen |
| advapi32.dll.RegQueryValueExW |
| advapi32.dll.RegOpenKeyExW |
| advapi32.dll.RegCloseKey |
| user32.dll.MessageBoxA |
| user32.dll.CharNextW |
| user32.dll.LoadStringW |
| kernel32.dll.Sleep |
| kernel32.dll.lstrlenW |
| kernel32.dll.VirtualQuery |
| kernel32.dll.QueryPerformanceCounter |
| kernel32.dll.GetTickCount |
| kernel32.dll.GetSystemInfo |
| kernel32.dll.GetVersion |
| kernel32.dll.CompareStringW |
| kernel32.dll.IsDBCSEadByteEx |

kernel32.dll.IsValidLocale

kernel32.dll.SetThreadLocale

kernel32.dll.GetSystemDefaultUILanguage

kernel32.dll.GetUserDefaultUILanguage

kernel32.dll.GetLocaleInfoW

kernel32.dll.WideCharToMultiByte

kernel32.dll.MultiByteToWideChar

kernel32.dll.GetConsoleOutputCP

kernel32.dll.GetConsoleCP

kernel32.dll.GetACP

kernel32.dll.LoadLibraryExW

kernel32.dll.GetStartupInfoW

kernel32.dll.GetProcAddress

kernel32.dll.GetModuleHandleW

kernel32.dll.GetModuleFileNameW

kernel32.dll.GetCommandLineW

kernel32.dll.FreeLibrary

kernel32.dll.GetLastError

kernel32.dll.UnhandledExceptionFilter

kernel32.dll.RtlUnwind

kernel32.dll.RaiseException

kernel32.dll.ExitProcess

kernel32.dll.ExitThread

kernel32.dll.SwitchToThread

kernel32.dll.GetCurrentThreadId

kernel32.dll.CreateThread

kernel32.dll.DeleteCriticalSection

kernel32.dll.LeaveCriticalSection

kernel32.dll.EnterCriticalSection

kernel32.dll.InitializeCriticalSection

kernel32.dll.FindFirstFileW

kernel32.dll.FindClose

kernel32.dll.SetCurrentDirectoryW

kernel32.dll.GetCurrentDirectoryW

kernel32.dll.RemoveDirectoryW

kernel32.dll.CreateDirectoryW

kernel32.dll.WriteFile

kernel32.dll.SetFilePointer

kernel32.dll.SetEndOfFile

kernel32.dll.ReadFile

kernel32.dll.GetFileType

kernel32.dll.GetFileSize

kernel32.dll.CreateFileW

kernel32.dll.GetStdHandle

kernel32.dll.CloseHandle

kernel32.dll.LoadLibraryA

kernel32.dll.TlsSetValue

kernel32.dll.TlsGetValue

kernel32.dll.LocalFree

kernel32.dll.LocalAlloc

user32.dll.SetClassLongW

user32.dll.GetClassLongW

user32.dll.SetWindowLongW
 user32.dll.GetWindowLongW
 user32.dll.CreateWindowExW

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
 HKEY_CURRENT_USER\Software\Embarcadero\Locales
 HKEY_LOCAL_MACHINE\Software\Embarcadero\Locales
 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\Software\Microsoft\Windows\Windows Error Reporting\WMR
 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
 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_CURRENT_USER\Control Panel\Desktop\WindowMetrics
 HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics\AppliedDPI
 HKEY_LOCAL_MACHINE\Software\Clients\Mail\Microsoft Outlook
 HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\DLLPathEx
 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_CURRENT_USER |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Sans Serif |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\523eb57157746d1459b46ffe5157ce084b427903.exe |
| 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 NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma |
| HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows |
| HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\device |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\SynchronousPrintHandleAccessMode |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ExtensionConfig\SspiCli |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\ExtensionConfig\SspiCli\CheckSignatureDll |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\ExtensionConfig\SspiCli\CheckSignatureRoutine |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SecurityProviders |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SspiCache |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Name |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Comment |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\Capabilities |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\SspiCache\credssp.dll\RpcId |

READ FILES

| |
|----------------------------------------------------------------------------------------------------------------------------|
| C:\Windows\System32\tzres.dll |
| \Device\KsecDD |
| C:\Windows\Fonts\staticcache.dat |
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Users\user\AppData\Local\Temp\523eb57157746d1459b46ffe5157ce084b427903.exe |
| C:\Windows\System32\uxtheme.dll.Config |
| C:\Windows\System32\uxtheme.dll |
| C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll |
| C:\Windows\WindowsShell.Manifest |
| C:\Users\user\AppData\Local\Temp\Sejour.INI |
| C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui |
| \\?\UNC\192.168.2.28\SQL2014\pipe\sql\query |
| C:\Program Files (x86)\Common Files\System\OLE DB\sqloledb.rll |
| C:\Program Files (x86)\Common Files\System\OLE DB\en-US\SQLLEDB.RLL.mui |
| C:\Windows\sysnative\spool\drivers\x64\3\mxdwdui.BUD |
| C:\Windows\sysnative\spool\drivers\x64\3\mxdwdui.gpd |
| C:\Windows\sysnative\spool\drivers\x64\3\STDNAMES.GPD |
| C:\Windows\sysnative\spool\drivers\x64\3\mxdwdui.ini |
| C:\Windows\sysnative\spool\drivers\x64\3\en-US\unires.dll.mui |
| C:\Windows\sysnative\spool\drivers\x64\3\en-US\univui.dll.mui |

MUTEXES

| |
|----------------------|
| CicLoadWinStaWinSta0 |
|----------------------|



Local\MSCTF.CtftMonitorInstMutexDefault1

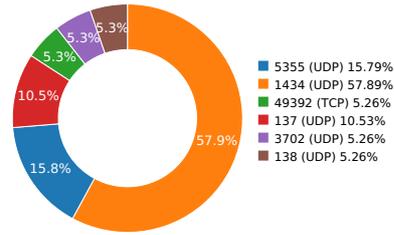
Local\WinSpl64To32Mutex_ed8f_0_3000

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



| Name | IP | Country | ASN | ASN Name | Trigger Process Type |
|------|---------------|---------------|-------|------------------------------------------------------------|----------------------|
| | 72.21.91.29 | United States | 15133 | MCI Communications Services, Inc. d/b/a Verizon Busines... | Malware Process |
| | 52.85.105.209 | United States | 16509 | Amazon Technologies Inc. | Malware Process |
| | 23.50.75.27 | United States | 3257 | Akamai Technologies, Inc. | Malware Process |

TCP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---------------------------------|-----------|--------------|-----------|
| 18.4309329987 | Sandbox | 192.168.56.7 | 49392 |

UDP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---------------------------------|-----------|-----------------|-----------|
| 7.15988397598 | Sandbox | 224.0.0.252 | 5355 |
| 7.20152616501 | Sandbox | 192.168.56.255 | 137 |
| 7.20219302177 | Sandbox | 224.0.0.252 | 5355 |
| 7.27732419968 | Sandbox | 239.255.255.250 | 3702 |
| 9.75390005112 | Sandbox | 224.0.0.252 | 5355 |
| 13.1890439987 | Sandbox | 192.168.56.255 | 138 |
| 14.1755170822 | Sandbox | 192.168.2.28 | 1434 |
| 37.4240560532 | Sandbox | 192.168.2.28 | 137 |
| 43.5360991955 | Sandbox | 192.168.2.28 | 1434 |
| 44.6419491768 | Sandbox | 192.168.2.28 | 1434 |
| 45.8455851078 | Sandbox | 192.168.2.28 | 1434 |
| 47.251401186 | Sandbox | 192.168.2.28 | 1434 |
| 49.0635421276 | Sandbox | 192.168.2.28 | 1434 |
| 51.0637819767 | Sandbox | 192.168.2.28 | 1434 |
| 53.0639560223 | Sandbox | 192.168.2.28 | 1434 |
| 55.0642511845 | Sandbox | 192.168.2.28 | 1434 |
| 57.0638020039 | Sandbox | 192.168.2.28 | 1434 |
| 59.0643200874 | Sandbox | 192.168.2.28 | 1434 |

DETAILED FILE INFO

CREATED / DROPPED FILES

| FILE PATH | TYPE AND HASHES |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\User\AppData\Local\Temp\Sejour.INI | Type : ASCII text, with CRLF line terminators MD5 : 1c78a603a75308f47a641de047aef53d SHA-1 : 8457e33b1ec46dbc19ee74f987476751af6dbc4c SHA-256 : da1ff283ffa1160ed63680aa7a77e78161d3250e52da96648a56f8df171bb5ba SHA-512 : 5d4fc8a1a10712a2fb3e1668f6d7948573998976da278f89ac7c07f8071e44b5f9de055 Size : 0.038 Kilobytes. |

MATCH YARA RULES

| MATCH RULES |
|-------------|
| |

STATIC FILE INFO

| | |
|--------------------------------------|---------------------------------------------------|
| File Name: | ResMonP.exe |
| File Type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| SHA1: | 523eb57157746d1459b46ffe5157ce084b427903 |
| MD5: | fabf007d0a26445c63be58cc1b0c5b70 |
| First Seen Date: | 2018-04-13 09:27:48.601084 (11 months ago) |
| Number Of Clients Seen: | 2 |
| Last Analysis Date: | 2018-04-13 09:27:48.601084 (11 months ago) |
| Human Expert Analysis Date: | 2018-04-13 12:20:15.445931 (11 months ago) |
| Human Expert Analysis Result: | Malware |

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

| PROPERTY | VALUE |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Magic Literal Enum | 3 |
| File Type Enum | 6 |
| Debug Artifacts | [] |
| Number Of Sections | 13 |
| Trid | [[52.9, u'Win32 Executable (generic)'], [23.5, u'Generic Win/DOS Executable'], [23.5, u'DOS Executable Generic']] |
| Compilation Time Stamp | 0x5A392412 [Tue Dec 19 14:37:06 2017 UTC] |
| LegalCopyright | San Bilgisayar ve Tic.Tur.Ith.Ihr.A.\xde. |
| InternalName | Sejour |
| FileVersion | 21.0.0.200 |
| CompanyName | San Bilgisayar ve Tic.Tur.Ith.Ihr.A.\xde. |
| PrivateBuild | |
| LegalTrademarks | Sejour |
| Comments | Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. |
| ProductName | Sejour |
| SpecialBuild | |
| ProductVersion | 21.0.0.200 |
| FileDescription | Sejour |
| OriginalFilename | Sejour.exe |
| Translation | 0x041f0x04e6 |
| Entry Point | 0x3eb6001 (.aspack) |
| Machine Type | Intel 386 or later - 32Bit |
| File Size | 14158848 |
| Ssdeep | 393216:g8Zky8P9JQ23oWTutSYP7pbW7u/xfAg4Q2wffjKoL:hky8P9NdTVAxWaj93hKoL |
| Sha256 | c23b180756ef6b5218d7a7493cd52467bbe3e476e5a06eeda0550b1aed875a07 |
| ExifInfo | [[u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'EXE:PrivateBuild': u'', u'SourceFile': u'nfs/fvs/valkyrie_shared/core/valkyrie_files/5/2/3/e/523eb57157746d1459b46ffe5157ce084b427903', u'EXE:OriginalFileName': u'Sejour.exe', u'EXE:ProductName': u'Sejour', u'EXE:InternalName': u'Sejour', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:04:13 09:23:15+00:00', u'EXE:InitializedDataSize': 21933568, u'File:FileModifyDate': u'2018:04:13 09:13:45+00:00', u'EXE:FileVersionNumber': u'21.0.0.200', u'EXE:FileVersion': u'21.0.0.200', u'File:FileSize': u'14 MB', u'EXE:CharacterSet': u'Windows, Turkish', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:LegalTrademarks': u'Sejour', u'EXE:ProductVersion': u'21.0.0.200', u'EXE:ObjectFileType': u'Executable application', u'EXE:SpecialBuild': u'', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'San Bilgisayar ve Tic.Tur.Ith.Ihr.A.\xde.', u'File:FileName': u'523eb57157746d1459b46ffe5157ce084b427903', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'.exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2017:12:19 14:37:06+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'San Bilgisayar ve Tic.Tur.Ith.Ihr.A.\xde.', u'EXE:LinkerVersion': 2.25, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'nfs/fvs/valkyrie_shared/core/valkyrie_files/5/2/3/e', u'EXE:FileDescription': u'Sejour', u'EXE:EntryPoint': u'0x3ab6001', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 34819584, u'EXE:Comments': u'Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.', u'File:FileNodeChangeDate': u'2018:04:13 09:13:45+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Turkish', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'21.0.0.200']] |
| Mime Type | application/x-dosexec |
| Imphash | 7993dd2895de4b607668c2b1643cc405 |

PE Sections

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---------|-----------------|--------------|----------|----------------|-----------------------------------|
| .text | 0x1000 | 0x20ec000 | 0x91d000 | 7.99994949567 | 240d297523696c417acfade9d2f5338 |
| .itext | 0x20ed000 | 0x4a000 | 0x11400 | 7.99476535014 | 17df7b3d8509101998988ed943875a87 |
| .data | 0x2137000 | 0x6e000 | 0x20200 | 7.99573512382 | 5b0579231860a93d34bba252c0a48dd5 |
| .bss | 0x21a5000 | 0x48ecf4 | 0x0 | 0.0 | d41d8cd98f00b204e9800998ecf8427e |
| .idata | 0x2634000 | 0xd000 | 0x3000 | 7.88802315736 | 0ae82b1a209c437514500a00d5d4d524 |
| .didata | 0x2641000 | 0x7000 | 0x1800 | 7.818433508 | 224ed3512f89e374ac8c0d400dfa192f |
| .edata | 0x2648000 | 0x1000 | 0x200 | 1.15857841712 | 67f95cb01f96bd6c6c9cd16ecd1f7962 |
| .tls | 0x2649000 | 0x64 | 0x0 | 0.0 | d41d8cd98f00b204e9800998ecf8427e |
| .rdata | 0x264a000 | 0x1000 | 0x200 | 0.276494917659 | f8f620caa4e03116cecd4720c8e76d14 |
| .reloc | 0x264b000 | 0x28e000 | 0x105400 | 7.99821064463 | 8ac4756b01ec6216eb58acfaad82bd96 |
| .rsrc | 0x28d9000 | 0x11dd000 | 0x322c00 | 7.96044488223 | 0477f21f8c96551618a7f0711d1be1f10 |
| .aspack | 0x3ab6000 | 0x6000 | 0x5600 | 4.0934954811 | 75cc98ad253a23fc8bdcdd5f337cbeaa |
| .adata | 0x3abc000 | 0x1000 | 0x0 | 0.0 | d41d8cd98f00b204e9800998ecf8427e |

PE Imports

- kernel32.dll
 - GetProcAddress
 - GetModuleHandleA
 - LoadLibraryA
- oleaut32.dll
 - SysFreeString
- advapi32.dll
 - RegQueryValueExW
- user32.dll
 - MessageBoxA
- user32.dll
 - SetClassLongW
- gdi32.dll
 - WidenPath
- version.dll
 - VerQueryValueW
- mpr.dll
 - WNetGetConnectionW
- advapi32.dll
 - RegUnLoadKeyW
- imagehlp.dll
 - ImageDirectoryEntryToData
- shfolder.dll
 - SHGetFolderPathW
- ole32.dll
 - CoCreateGuid
- oleaut32.dll
 - SafeArrayPtrOfIndex
- oleaut32.dll
 - CreateErrorInfo
- ole32.dll
 - CreateStreamOnHGlobal
- comctl32.dll
 - InitializeFlatSB
- user32.dll
 - EnumDisplayMonitors
- msvcrt.dll
 - isxdigit
- shell32.dll
 - SHFileOperationW
- wininet.dll
 - HttpSendRequestExW
- shell32.dll
 - SHGetSpecialFolderLocation
- comdlg32.dll
 - PrintDlgW
- winspool.drv
 - WritePrinter
- winspool.drv
 - GetDefaultPrinterW
- gdi32.dll
 - TranslateCharSetInfo
- wsock32.dll
 - _WSAFDIsSet
- gdi32.dll
 - SetLayout
- winspool.drv
 - DocumentPropertiesW
- winmm.dll
 - timeGetTime
- fontsub.dll
 - CreateFontPackage
- usp10.dll
 - ScriptShape
- gdiplus.dll
 - GdiipGetPenFillType
- oleacc.dll
 - LresultFromObject
- oledlg.dll
 - OleUIObjectPropertiesW
- gdiplus.dll
 - GdiipEmfToWmfBits
- netapi32.dll
 - Netbios
- gdi32.dll
 - TranslateCharSetInfo
- usp10.dll
 - ScriptPlace

PE Exports

TMethodImplementationIntercept

PE Resources

- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'ACUPG', u'offset': 42960332, u'sha256': u'6a76075bd209f459583fbbc72f1dfac9031db0958ea0bb02342c89da205cb662', u'type': u'data', u'size': 9216)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'DXSkins', u'offset': 42969548, u'sha256': u'74c3c92d2a8ba07d29b48960b591c2191e0966e2c96621078ef7021b04a94b89', u'type': u'data', u'size': 2970)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'DXSkins', u'offset': 42972520, u'sha256': u'aa601726bfd3809f6a1a3e87b882381e5d9b2b7b92aa4d60dff14b2a2a8aa4dd', u'type': u'data', u'size': 841)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42973364, u'sha256': u'05f82108fe5f19bd9c739a3ba6ee4893ed042fb3549850474567c0f51f7859a4', u'type': u'data', u'size': 207)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42973572, u'sha256': u'3bd57ca60d9e7873a47cd488051a32b031a9d4093cd6c8cf64b771519b6f4ab6', u'type': u'data', u'size': 183)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42973756, u'sha256': u'466173cf5402698ea42f6eacfd9661c675a4434992168b4253cafb99cb946b6c', u'type': u'data', u'size': 216)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42973972, u'sha256': u'5ecc6120e49186c1cc683207f8ecee28603b5816c631e7fceb3307af058ecc6', u'type': u'data', u'size': 227)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42974200, u'sha256': u'd32259a7f7db4c2865818bf2696494e40339cea5e16afa4ec784c0768d9a85b9a', u'type': u'data', u'size': 160)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42974360, u'sha256': u'23a328d8f0dd026dc3b4d715951483867e06c5e115d28d591c74fa186f280814', u'type': u'data', u'size': 164)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42974524, u'sha256': u'68577fb20829cf572cb98c844a3c9b7bde95be33900c699aad833dc419c561bf5', u'type': u'data', u'size': 168)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42974692, u'sha256': u'ab3ba6a9b602a63a955e4344b1acd488f5c376381042eb92901c9105940a6814', u'type': u'data', u'size': 171)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42974864, u'sha256': u'f231a7d60a2bea789336ff3da1ef6fc4cbd31a9e6bb77453a884ddd4642eb79', u'type': u'data', u'size': 189)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42975056, u'sha256': u'74503c7adfb53efced24ca8047479c747508810b511dcd9e9ea80e7ec836a5d', u'type': u'data', u'size': 190)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42975248, u'sha256': u'1e3c396ca9c21c58057750a2d57cd75fff7e49194ff55f276a6da4f240bd76d7', u'type': u'data', u'size': 170)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42975420, u'sha256': u'12d2cfa388f5f7b9a9e4f0dbe46633f3a50ca12e0444cbc7309000da4ec7341', u'type': u'data', u'size': 175)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42975596, u'sha256': u'dd10bd2c7af7e6024486bbe07997787367f78cf31ec8d43f4000124a0f57247b', u'type': u'data', u'size': 244)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42975840, u'sha256': u'5d35e3a4e55ed1a930b463c9364a77246182b7bc1e8c9dcdfaf4357d4f3c6c1d', u'type': u'data', u'size': 196)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'PNG', u'offset': 42976036, u'sha256': u'c2f21fa5d1ba8df2e3a2d7af360231edbbe7b928e2f96c938320482230040bfd', u'type': u'data', u'size': 1746)
- 🔗 (u'lang': u'LANG_ENGLISH', u'name': u'GIF', u'offset': 42977784, u'sha256': u'195eea48830a1e02145f95afb56ff312340e27cda2027cd0564c5994a62d10f2', u'type': u'data', u'size': 726)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'PNG', u'offset': 42978512, u'sha256': u'9e9f2565796dc851a676eb57f13a811fcdcc3936188477bcaca2a2fb0637df8', u'type': u'data', u'size': 4778)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'PNG', u'offset': 42983292, u'sha256': u'51f0a4d048521354b83a32a8051643f8c1b792d7cc8c25350cd9bf0afd4f5ed9', u'type': u'data', u'size': 972)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'PNG', u'offset': 42984264, u'sha256': u'ac6a96738612f46553ce4535bc5d1cf441bf4df624adef0c58b33b382e5fbd', u'type': u'data', u'size': 164)
- 🔗 (u'lang': u'LANG_NEUTRAL', u'name': u'PNG', u'offset': 42984428, u'sha256': u'bac8c69eb1a40e49e5dc31c6190c93d586721080de67838a35aec7cf43fa06f', u'type': u'data', u'size': 281)

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559132, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559152, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559172, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559192, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559212, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559232, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 61559252, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 61559272, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_RUSSIAN', u'name': u'RT_GROUP_CURSOR', u'offset': 61559292, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559312, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 61559332, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559352, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559372, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559392, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559412, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559432, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559452, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559472, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 61559492, u'sha256': u'de47c9b27eb8d300dbb5f2c353e632c393262cf06340c4fa7f1b40c4cbd36f90', u'type': u'data', u'size': 20}
 {u'lang': u'LANG_TURKISH', u'name': u'RT_GROUP_ICON', u'offset': 61570772, u'sha256': u'48f5b51a94179143e7e3b8941169a7e911f09017986995d040446967ad9e76f', u'type': u'MS Windows icon resource - 1 icon, 32x32', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 61570752, u'sha256': u'4c53fd5f3f97d57788a4486fb2990f2ce2ea49ead439709428feda69a58f26d', u'type': u'MS Windows icon resource - 1 icon, 30x30', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 61570732, u'sha256': u'03f3c5ecd5a1d11bc0fb01fda97f81c2894ec1778e3b878f9d27506263923846', u'type': u'MS Windows icon resource - 1 icon, 30x30', u'size': 20}
 {u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 61570712, u'sha256': u'ce661a77befb715b41c454a9fd8b7bd72e020fca0638c7af037b92a38c6108e1', u'type': u'MS Windows icon resource - 1 icon, 30x30', u'size': 20}
 {u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 61570692, u'sha256': u'7a08031f75135d4fae812d5b19935e247b7f02af232e35930c40ea355f10d2', u'type': u'MS Windows icon resource - 1 icon, 32x32, 16 colors', u'size': 20}
 {u'lang': u'LANG_TURKISH', u'name': u'RT_VERSION', u'offset': 61569180, u'sha256': u'7df77cc30240fbd4ff4cc683f6d6395f608b6b78f0217dd0876dd8f1547ccb24', u'type': u'data', u'size': 1512}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: ODAAdı, Bölge: BOAdı, Operatör: OPAdı, Voucher: İpinde ara, Rez. Statüsü: Balon, Rez. Tipi: Seçim Yok, Asıl Voucher: İpinde ara

Oda: Oda Tipi, Pansiyon, Otel / Operatör Konfirmasyonu, Otel Konf. Tar., Opr. Konf. Tar., Vch. İlk Baskı, Vch. Son Baskı, Grubu, Konfirmasyon No

Giriş Tarihi, Çıkış Tarihi, Gelış Tarihi, Dönüş Tarihi, Otel Alış Tarihi, Opr. Satış Tarihi, Kayıt Tarihi

Hotel2S Sejour'la Entegre | H2S Otellerine hatırlatma gün

Liste Şekli: Rezervasyon Özet, Rezervasyon Detay, Müşteri Özet

Gruplama Seçenekleri: Operatör, Voucher, Otel, Giriş Tarihi, Çıkış Tarihi, Gelış Tarihi, Uçuş, Gelış Trf. Tarihi, Dönüş Trf. Tarihi

Tüm Rezervasyonlar

523eb57157746d1459...

Computer

523eb57157746d1459b46ffe5157ce084b427903

[DBNETLIB][ConnectionOpen (Connect)].SQL Server does not exist or access denied.

OK

523eb57157746d1459...

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: ODAAdı, Bölge: BOAdı, Operatör: OPAdı, Voucher: İpinde ara, Rez. Statüsü: Balon, Rez. Tipi: Seçim Yok, Asıl Voucher: İpinde ara

Oda: Oda Tipi, Pansiyon, Otel / Operatör Konfirmasyonu, Otel Konf. Tar., Opr. Konf. Tar., Vch. İlk Baskı, Vch. Son Baskı, Grubu, Konfirmasyon No

Giriş Tarihi, Çıkış Tarihi, Gelış Tarihi, Dönüş Tarihi, Otel Alış Tarihi, Opr. Satış Tarihi, Kayıt Tarihi

Hotel2S Sejour'la Entegre | H2S Otellerine hatırlatma gün

Liste Şekli: Rezervasyon Özet, Rezervasyon Detay, Müşteri Özet

Gruplama Seçenekleri: Operatör, Voucher, Otel, Giriş Tarihi, Çıkış Tarihi, Gelış Tarihi, Uçuş, Gelış Trf. Tarihi, Dönüş Trf. Tarihi

Tüm Rezervasyonlar

523eb57157746d1459...

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Gelış Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Gelış Tarihi Uçuş Gelış Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:02 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Gelış Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Gelış Tarihi Uçuş Gelış Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:01 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Gelış Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Gelış Tarihi Uçuş Gelış Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:03 PM

Sejour Rezervasyon Monitörü

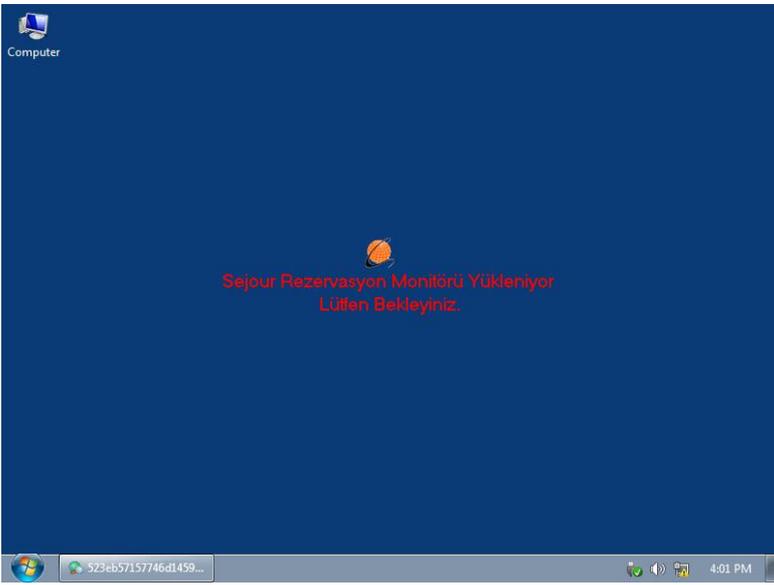
Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: [DAdı] Giriş Tarihi: [] / [] / [] Otel / Operatör Konfirme: []
Bölge: [BoAdı] Oda Tipi: [] Çıkış Tarihi: [] / [] / [] Otel Konf. Tar.: [] / [] / []
Operatör: [OpAdı] Pansiyon: [] Geliş Tarihi: [] / [] / [] Opr. Konf. Tar.: [] / [] / []
Voucher: [] İpinde ara Opr. Fiy. Filtresi: [Hepsi] Dönüş Tarihi: [] / [] / [] Vch. İlk Baskı: [] / [] / []
Rez. Statüsü: [] Balon: [Hepsi] Otel Alış Tarihi: [] / [] / [] Vch. Son Baskı: [] / [] / []
Rez. Tipi: [Seçim Yok] Pasif: [Hepsi] Opr. Satış Tarihi: [] / [] / [] Grubu: []
Asıl Voucher: [] İpinde ara Kayıt Tarihi: [] / [] / [] Konfirme No: []
Hotel25 Sejour'la Entegre: [Hepsi] H25 Otellerine hakikatma gün

Liste Şekli: [Rezervasyon Özeti] [Rezervasyon Detay] [Rezervasyon Detay2] [Müşteri Detay] [Müşteri Detay2]
Gruplama Seçenekleri: [Operator] [Voucher] [Otel] [Giriş Tarihi] [Çıkış Tarihi] [Geliş Tarihi] [Uçuş] [Geliş Trf. Tarihi] [Dönüş Trf. Tarihi]
Geliş: []

| Rez. Tipi | Son Deg. Tar. | Son Değişiklik | Tip | Operatör | Operatör Adı |
|----------------------|---------------|----------------|-----|----------|--------------|
| <No data to display> | | | | | |

Tüm Rezervasyonlar



Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: S23eb57157746d1459... 4:03 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: S23eb57157746d1459... 4:03 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: S23eb57157746d1459... 4:03 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:02 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:02 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara Kayıt Tarihi: Konfirme No:

Hotel2S Sejour'la Entegre: H2S Otellerine hatırlama gün:

Liste Sektörü: Rezervasyon Özet Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özet Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:01 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara: Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Hepsisi: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Seçim Yok: Pasif: Hepsisi: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara: Kayıt Tarihi: Konfirme No:

Hotel2Sejour'la Entegre: H25 Otellerine hakılatma gün:

Liste Şekli: Rezervasyon Özeti Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özeti Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows taskbar: 523eb57157746d1459... 4:02 PM

Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirme:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Geliş Tarihi: Opr. Konf. Tar.:

Voucher: İpinde ara: Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Hepsisi: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Seçim Yok: Pasif: Hepsisi: Opr. Satış Tarihi: Grubu:

Asıl Voucher: İpinde ara: Kayıt Tarihi: Konfirme No:

Hotel2Sejour'la Entegre: H25 Otellerine hakılatma gün:

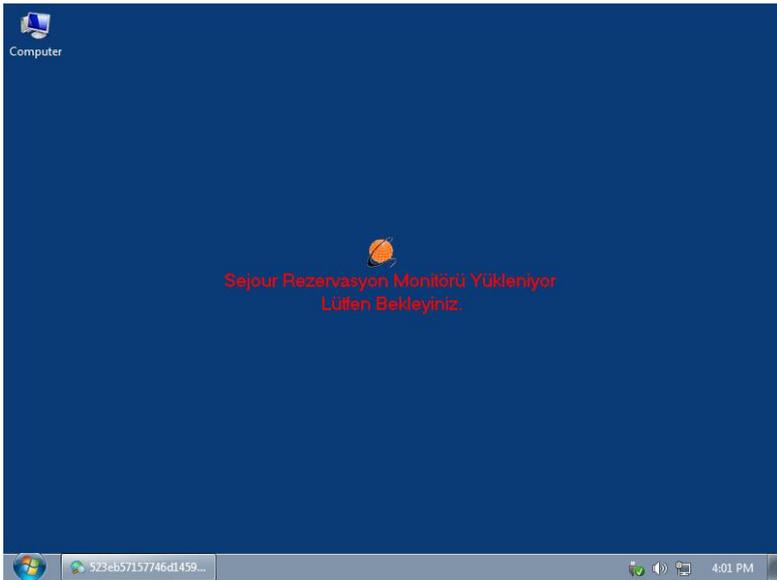
Liste Şekli: Rezervasyon Özeti Rezervasyon Detay Rezervasyon Detay-2 Müşteri Özeti Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Geliş Tarihi Uçuş Geliş Trf. Tarihi Dönüş Trf. Tarihi

Geliş:

Tüm Rezervasyonlar

Windows taskbar: 523eb57157746d1459... 4:03 PM



Sejour Rezervasyon Monitörü

Rezervasyon Kriterleri | Rezervasyon Kriterleri 2 | Müşteri Kriterleri | Renklendirme | Fatura Parametreleri

Otel: Oda: Giriş Tarihi: Otel / Operatör Konfirmasyonu:

Bölge: Oda Tipi: Çıkış Tarihi: Otel Konf. Tar.:

Operatör: Pansiyon: Gelış Tarihi: Opr. Konf. Tar.:

Voucher: Opr. Fiy. Filtresi: Dönüş Tarihi: Vch. İlk Baskı:

Rez. Statüsü: Balon: Hepsisi: Otel Alış Tarihi: Vch. Son Baskı:

Rez. Tipi: Pasif: Hepsisi: Opr. Satış Tarihi: Grubu:

Asıl Voucher: Kayıt Tarihi: Konfirmasyon No:

Hotel2S Sejour'la Entegre: H2S Otellerine hakikatma gün:

Liste Şekli: Rezervasyon Özeti Rezervasyon Detay Rezervasyon Detay2 Müşteri Detay Müşteri Detay

Gruplama Seçenekleri: Operatör Voucher Otel Giriş Tarihi Çıkış Tarihi Gelış Tarihi Uçuş Gelış Trf. Tarihi Dönüş Trf. Tarihi

Gruplama:

| Rez. Tipi | Son Deg. Tar. | Son Değişiklik | Tip | Operatör | Operatör Adı |
|----------------------|---------------|----------------|-----|----------|--------------|
| <No data to display> | | | | | |

Tüm Rezervasyonlar

Windows Taskbar: 523eb57157746d1459... 4:04 PM