Taleret strings - APT (1)

contagioexchange.blogspot.com/2013/08/taleret-strings-apt-1.html

File: Taleret_FED166A667AB9CBB1EF6331B8E9D7894
MD5: fed166a667ab9cbb1ef6331b8e9d7894
Size: 36864

Ascii Strings:

!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.reloc
----------snip
MFC42.DLL
_beginthreadex
strstr
printf
fclose
fprintf
_strdate
_strtime
fopen
_vsnprintf
strchr
rand
srand
time
__CxxFrameHandler
strrchr
sprintf
fread
_mbscmp
free
malloc
MSVCRT.dll
_initterm

_adjust_fdiv
GetProcAddress
LoadLibraryA
ExitProcess
Sleep
WaitForSingleObject
FreeConsole
ExpandEnvironmentStringsA
GetLocalTime
GetLastError
CloseHandle
GetCurrentProcess
LocalFree
HeapFree
HeapAlloc
GetProcessHeap
Process32Next
OpenProcess
Process32First
CreateToolhelp32Snapshot
DeleteFileA
FreeLibrary
ReadFile
SetFilePointer
GetFileSize
GetTickCount
OutputDebugStringA
KERNEL32.dll
PostQuitMessage
DefWindowProcA
DispatchMessageA
TranslateMessage
GetMessageA
UpdateWindow
ShowWindow
CreateWindowExA
RegisterClassA
LoadCursorA
LoadIconA
SendMessageTimeoutA
USER32.dll
GetStockObject

GDI32.dll
RegisterServiceCtrlHandlerW
SetServiceStatus
RegQueryValueExA
RegCloseKey
AdjustTokenPrivileges
LookupPrivilegeValueA
ConvertSidToStringSidA
EqualSid
GetTokenInformation
ADVAPI32.dll
InternetCloseHandle
InternetSetOptionA
InternetSetCookieA
HttpQueryInfoA
InternetConnectA
HttpSendRequestA
HttpOpenRequestA
WININET.dll
GetAdaptersInfo
iphlpapi.dll
SHRegGetValueA
SHLWAPI.dll
CoCreateGuid
ole32.dll
_strlwr
_strnicmp
MsgHandlerDll.dll
ServiceMain
Start
wxxxd
kernel32.dll
CreateDirectoryA
GetWindowsDirectoryA
WinExec
GetDriveTypeA
GetFileAttributesA
GetLogicalDriveStringsA
DeleteFileA
MoveFileA
FindNextFileA
FindFirstFileA

FindResourceA
CreateFileA
GetVolumeInformationA
CopyFileA
CreateMutexA
GetTempPathA
lstrcatA
lstrcpyA
lstrcmpA
user32.dll
GetWindowTextA
GetForegroundWindow
FindWindowExA
PostMessageA
GetCursorPos
WindowFromPoint
wsprintfA
keybd_event
GetParent
ADVAPI32.dll
RegSetValueExA
RegCreateKeyA
RegEnumKeyA
RegDeleteKeyA
RegSetValueA
RegOpenKeyExA
RegQueryValueA
RegQueryValueExA
RegDeleteValueA
CreatePipe
GetSystemDirectoryA
CreateProcessA
User32.dll
SetWindowsHookExA
CallNextHookEx
CreateFileMappingA
GetModuleFileNameA
Wininet.dll
InternetOpenA
InternetOpenUrlA
HttpQueryInfoA
InternetReadFile

Advapi32.dll
RegCreateKeyExA
OpenProcessToken
rundll32.exe
The Window
sdfjx
https:
MSIE 6.0; Windows NT 5.1; SV1)
Mozilla/4.0 (compatible;
Software\Microsoft\Windows\CurrentVersion\Internet Settings
User Agent
XXXXX
%s %s - %s
ail: %s:%d
conn f
read from registry
Software\Microsoft\SysInternal
furl: %s
auto proxy
%tmp%\~alot.dat
1A10
{AEBA21FA-782A-4A90-978D-B72164C80120}
{A8A88C49-5EB2-4990-A1A2-0876022C854F}
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
DefaultConnectionSettings
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
explorer.exe
SeDebugPrivilege
MUID
http://%s:%d
http://%s
NOT Certified
AFTER: Disconnect
AFTER: %d s
SetTime: %d OK
SendFile: %d OK
%temp%\
WRONG PASSWORD
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
 error:
 Run
 Run error

Run OK
ShellExecuteA
shell32.dll
%%temp%%\%u
/webhp?source=
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Content-Type: application/x-www-form-urlencoded
POST
HTTP/1.1
%02X-%02X-%02X-%02X-%02X-%02X
0.0.0.0
01-01-01-01-01-01
%04x
%04x%04x%04x%04x
0#0(0A0F0L0S0X0q0v0|0
11161<1C1H1a1f1l1s1x1
2!2&2,23282Q2V2\2c2h2
3#3(3A3F3L3S3X3q3v3|3
41464<4C4H4a4f4l4s4x4
5!5&5,53585Q5V5\5c5h5
6#6(6A6F6L6S6X6q6v6|6
71767<7C7H7a7f7l7s7x7
8!8&8,83888Q8V8\8c8h8
9#9(9A9F9L9S9X9{9
:":.:E:P:a:w:
;#;);=;C;I;O;
<1<]<}<
=,=1=D=M=y=
>;>Z>
474F4O4V4]4y4
5,5O5[5k5
6 6?6k6v6
9O9U9d9v9
:6:=:^:e:w:
;0;e;
< <0<=<t<
<#=:=^=
>_>f>
?7?O?
0]0l0
1Q1V1\1c1h1
2#2(232

767p7
9X:I:
=!>+><>C>W>
>`?q?
1<2S2
3"3(353<3w3
5=5P5
6<6A6G6Z6
6/767D7|7
9c:h:q:
;4;F;R;g;
<2=H=
?8?Y?j?t?
0.030>0N0X0b0q0w0
1 1&1,12181>1D1J1P1V1\1b1
2+272=2_2q2
4G4Y4
4V5y5
2$2,242<2D2L2T2\2d2l2x2
3(3D3P3l3t3|3
4 4<4D4L4X4t4|4
0 0$0(0,0004080<0@0D0H0L0P0T0X0\0`0d0h0l0p0t0x0|0

Unicode Strings:
