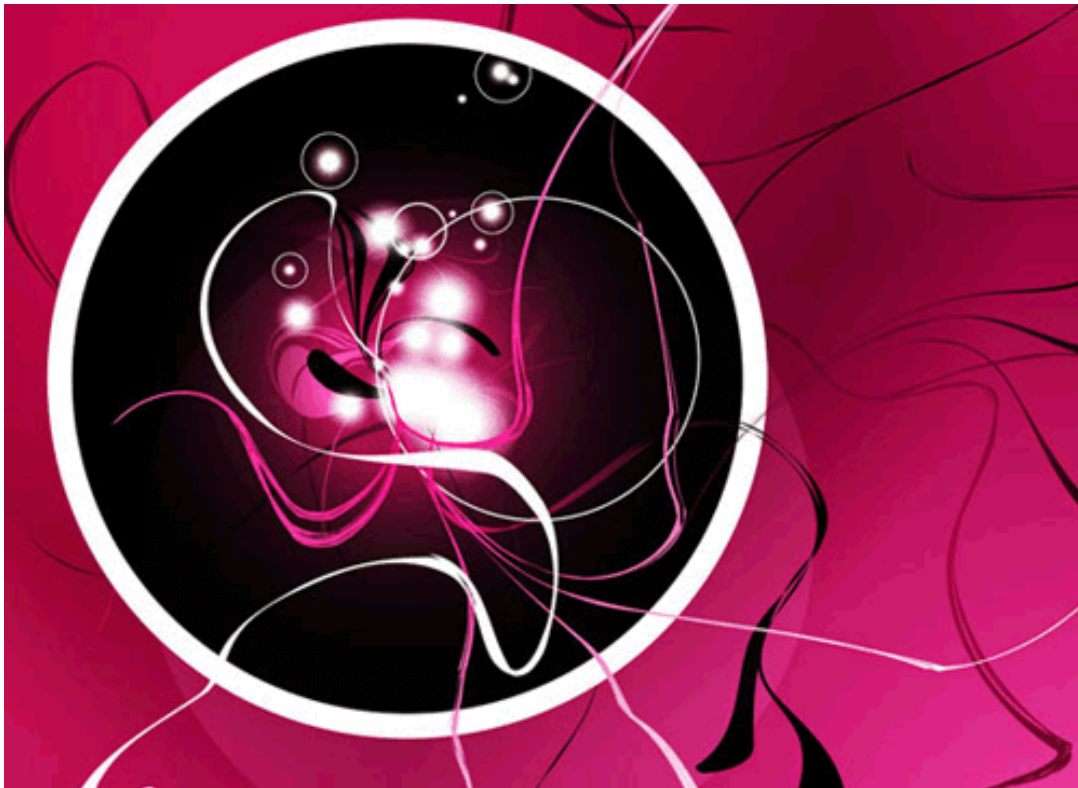


Analysis of Small.R.Virus



Written By Dash Shendy <admin@dash.za.net>
25th August 2009

Contents

1. INTRODUCTION
2. TESTING ENVIRONMENT
3. STATIC ANALYSIS
4. DYNAMIC ANALYSIS
5. CONCLUSION
6. REMOVAL INSTRUCTIONS
7. RECOMMENDATIONS
8. REFERENCES

INTRODUCTION

A friend of mine brought me some music on his flash drive, I plugged it into my usb port and my Anti-Virus freaked out at the autorun.inf contained on it, so I proceeded to examine and analyze the malware. My Anti-Virus labeled it as Win32/Small.R.Virus, what follows is my analysis of the binary I found.

TESTING ENVIRONMENT

I will be testing the executable in a Virtual Machine Environment.

Tools I will be using:

- OllyDbg 1.10
- FileMon by Sysinternals
- RegMon by Sysinternals
- hashcalc

STATIC ANALYSIS

Size:

104KB (106,496 bytes)

MD5:

cdf570f207662c7da9cc69c164ec24f6

SHA1:

a820630017b56be9fbf18ba6c8e279d24849b9fe

SHA256:

671e85788246990bdcd220ea79ce5cfe6298120e2668672e6073162010
3c80b6

Original Filename:

INFO.EXE

Magic File Type:

MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit

Packer Signature:

N/A

Anti-Virus Results:

Results from

<http://www.virustotal.com/analysis/671e85788246990bdcd220ea79ce5cfe6298120e2668672e60731620103c80b6-1246408312>

a-squared	Virus.Win32.Small!IK
AhnLab-V3	Win-Trojan/Xema.106496.F
AntiVir	TR/Agent.Small.D.2
Antiy-AVL	Virus/Win32.Small.gen
Authentium	W32/TrojanX.IQC
Avast	Win32:Small-EAE
AVG	Worm/AutoRun.M
BitDefender	Trojan.Agent.Small.D
CAT-QuickHeal	Worm.Small.r
ClamAV	W32.Silly
Comodo	Win32.Small.R
DrWeb	Win32.HLLW.Ofni
eSafe	Virus.Win32.Small.r
eTrust-Vet	Win32/Enfomend.A
F-Prot	W32/TrojanX.IQC
F-Secure	Virus.Win32.Small.r
Fortinet	W32/SillySvc.J!tr.bdr
GData	Trojan.Agent.Small.D
Ikarus	Virus.Win32.Small
Jiangmin	Backdoor/Small.dw
K7AntiVirus	Worm.Win32.Small
Kaspersky	Virus.Win32.Small.r
McAfee	Generic BackDoor.j
McAfee+Artemis	Generic BackDoor.j
McAfee-GW-Ed	Trojan.Agent.Small.D.2
Microsoft	Trojan:Win32/Small
NOD32	Win32/Small.R
Norman	W32/Smalldoor.AOLQ
nProtect	Trojan/W32.Agent.106496.B
Panda	Trj/Agent.FQZ
PCTools	Trojan.Agent.WXQ
Prevx	High Risk Cloaked Malware
Rising	Worm.Agent.fc
Sophos	W32/SillyFDC-H
Sunbelt	Bulk Trojan
Symantec	W32.SillyDC
TheHacker	Trojan/Small.r
TrendMicro	WORM_SMALL.HYN
VBA32	Trojan.Win32.Small

ViRobot
VirusBuster

Trojan.Win32.Small.106496
Trojan.Agent.LXZD

Kernel32.dll Imports:

The file INFO.EXE imports the following functions from kernel32.dll

CloseHandle	CompareStringA
CompareStringW	CopyFileW
CreateDirectoryW	CreateFileW
CreateProcessW	CreateThread
DeleteCriticalSection	DeleteFileW
EnterCriticalSection	EnumSystemLocalesA
ExitProcess	ExitThread
FatalAppExitA	FindClose
FindFirstFileW	FindNextFileW
FlushFileBuffers	FreeEnvironmentStringsA
FreeEnvironmentStringsW	GetACP
GetCPIInfo	GetCommandLineA
GetCurrentDirectoryW	GetCurrentDirectoryW
GetCurrentProcess	GetCurrentProcessId
GetCurrentThread	GetCurrentThreadId
GetDateFormatA	GetDriveTypeW
GetEnvironmentStrings	GetEnvironmentStringsW
GetFileType	GetLastError
GetLocalTime	GetLocaleInfoA
GetLocaleInfoW	GetLogicalDrives
GetModuleFileNameA	GetModuleFileNameW
GetModuleHandleA	GetOEMCP
GetProcAddress	GetStartupInfoA
GetStartupInfoW	GetStdHandle
GetStringTypeA	GetStringTypeW
GetSystemDirectoryW	GetSystemInfo
GetSystemTimeAsFileTime	GetTickCount
GetTimeFormatA	GetTimeZoneInformation
GetUserDefaultLCID	GetVersionExA
GlobalAddAtomW	GlobalDeleteAtom
GlobalFindAtomW	HeapAlloc
HeapCreate	HeapDestroy
HeapFree	HeapReAlloc
HeapSize	InitializeCriticalSection
InterlockedExchange	IsBadCodePtr
IsBadReadPtr	IsBadWritePtr
IsValidCodePage	IsValidLocale
LCMapStringA	LCMapStringW

LeaveCriticalSection	LoadLibraryA
MoveFileExW	MultiByteToWideChar
QueryPerformanceCounter	RaiseException
ReadFile	RtlUnwind
SetConsoleCtrlHandler	SetCurrentDirectoryW
SetEndOfFile	SetEnvironmentVariableA
SetErrorMode	SetFileAttributesW
SetFilePointer	SetHandleCount
SetLastError	SetStdHandle
SetUnhandledExceptionFilter	Sleep
TerminateProcess	TlsAlloc
TlsFree	TlsGetValue
TlsSetValue	UnhandledExceptionFilter
VirtualAlloc	VirtualFree
VirtualProtect	VirtualQuery
WideCharToMultiByte	WriteFile

User32.dll Imports:

The file INFO.EXE imports the following functions from User32.dll

wsprintfW

Advapi32.dll Imports:

The file INFO.EXE imports the following functions from Advapi.dll

RegOpenKeyExW
RegSetValueExW

DYNAMIC ANALYSIS

Characteristics:

Upon execution:

- it copies and renames itself to C:\Windows\System\svchost.exe which then runs as the currently logged-in user, after which the parent process (INFO.EXE) exits.
- It creates the directory C:\Windows\System_sv_CMD_
- It Add the following registry entry to survive reboot:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
Userinit =userinit.exe,C:\Windows\System\svchost.exe

- It starts another thread that loops thru drives A to Z and as soon as a REMOVABLE drive (e.g. Flash Drive) is present in the system, it copies itself to it at this location:
<DriveRoot>\RECYCLER\INFO.exe
- It Also copies the following autorun.inf file to the REMOVABLE Drive Root in order to spread via REMOVABLE Drives.
[autorun]
open=
shell\open\Command=RECYCLER\INFO.exe
shell\open\Default=1
shell\explore\Command=RECYCLER\INFO.exe
- It also loads the following dlls into its address space:
RCPRT4.dll Secur32.dll ntdll.dll gdi32.dll
- Svchost.exe terminates if executed by itself.

CONCLUSION

We have seen how this malware can spread itself by using the autorun feature of REMOVABLE Drives, as well as copying itself to a different location and disguising itself as the Generic Windows Process called svchost.exe.

REMOVAL INSTRUCTIONS

1. Terminate svchost.exe (The one that runs as the logged-in user).
2. Delete the directory C:\WINDOWS\SYSTEM32_sv_CMD_
3. Remove the start-up entry found under
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
Set Userinit = userinit.exe
4. Format your flash drive if infected.
5. It is also a good idea to run "sfc /scannow" to check windows files' integrity (You will need a Windows CD for this).

GENERAL RECOMENDATIONS

To help better your chances against malware:

- Always keep your OS patch levels up-to-date.
- Scan with a regularly updated Anti-Virus
- Scan with latest Anti-Rootkit tools
- Use a network (not host!) firewall to block outbound connections to non-standard ports and filter traffic coming in.
- Turn off and remove unneeded services.
- Turn off the Autorun feature on all removable drives.

REFERENCES

- Virus Total
<http://www.virustotal.com/>
- OllyDbg 1.10
<http://www.ollydbg.de/>
- FileMon by SysInternals (Now MS)
<http://technet.microsoft.com/en-us/sysinternals/bb896642.aspx>
- RegMon by SysInternals (Now MS)
<http://technet.microsoft.com/en-us/sysinternals/bb896652.aspx>
- hashcalc by SlavaSoft
<http://www.slavasoft.com/hashcalc/index.htm>