

Part 1

Basic Static Analysis

How to retrieve information without executing the malware and form a quick hypothesis about what it is doing

PE header, imported libraries, functions, strings, etc.

IoC are important for hypothesis building

IoC – Indicator of compromise

Will be used for any artifact that indicate that we may be facing malicious code

- Malware analysis can provide valuable IoC
- Often used to build IDS signatures
- Good IoC's can be helpful
- Bad IoC's can be a waste of time
- Maximizing true positive (what we want)
Minimizing false positives (waste of time)

True Positive	False Positive
True Negative	False Negative

Basic Static Analysis

How and where can we “quickly” find IoC’s ?

- Anti-Virus, Virus Total
- Hash and fuzzy hash
- Packed and obfuscated
- Portable Executable (PE) File Format
- Strings
- Linked libraries and functions (Imports and exports)

Challenge 1

- Use information available through basic static analysis techniques
- Describe potential indicators of compromise (IoC's) and use them to form a hypothesis about the potential purpose/functionality of the sample

Suggested Approach

- Choose to use PeStudio – look for IoCs
NB! Results are version dependent
(8.42 vs 8.54)

Indicators from PeStudio

- Hash
- Indicators (13/21 – indicates malicious)
- File header – TimeDateStamp
- Sections: .bbs? Raw size vs virtual size?
- Imported Libraries
What functionality do these libraries and functions potentially give?
 - Network (WSAStartup, connect, bind, ...)
 - GetTickCount (anti-debug?)
 - Mutex (CreateMutex)
 - Process (Create/terminate Process/thread, ShellExecute)
 - Keys (GetAsynkKeyState, GetKeyState)
 - Registry (open, create, ...)
 - File (open create, ...)
- Strings (wuamqr.exe, krnel, keylog.txt)
- Version: original filename – wuaumgr.exe

File Help



- ▶ c:\users\rem\desktop\spybot.exe
- Indicators (13/21)
- ▶ Virustotal (lookup failed)
- DOS Stub (64 bytes)
- DOS Header (64 bytes)
- File Header (20 bytes)
- Optional Header (224 bytes)
- Directories (2/15)
- Sections (5)
- Imported Libraries (2/7)
- Imported Symbols (72/110)
- Exported Symbols (0)
- Exceptions (0)
- Relocations (0)
- Certificates (0)
- Thread Local Storage (n/a)
- Resources (3)
- Strings (3/247)
- Debug (n/a)
- Manifest (n/a)
- Version (1/12)
- Overlay (Unknown)

Property	Value
Signature	0x00004550
Machine	0x014C (CPU type I386 (or higher))
NumberOfSections	5
TimeDateStamp	0x3E9DE2A5 (Wed Apr 16 19:09:2...
PointerToSymbolTable	0x00000000
NumberOfSymbols	0x00000000
SizeOfOptionalHeader	0x00E0 (224 bytes)
Characteristics	0x010E
32bit Processor	true
Relocation stripped	false
Large Address Aware	false
Uniprocessor	false
System Image	false
Dynamic-link library	false
Executable	true
Debug information stripped	false
If on a Network, copy and run from the swap	false
If on a Removable Media, copy and run fro...	false

Property	Value	Value	Value	Value	Value
Name	.text	.bss	.data	.idata	.rsrc
Virtual Size (bytes)	0x00006F54 (28500)	0x000093C4 (37828)	0x00001D24 (7460)	0x00000D68 (3432)	0x00000D68 (3432)
Virtual Address	0x00001000	0x00008000	0x00012000	0x00014000	0x00015000
Raw Size (bytes)	0x00006F54 (28500)	0x00000000 (0)	0x00001D24 (7460)	0x00000D68 (3432)	0x00000D68 (3432)
Raw Address	0x00000400	0x00000000	0x00007400	0x00009200	0x0000A000
PointerToRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
PointerToLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfLinenumbe...	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
Entry Point	x	-	-	-	-
MD5	1450CC5ECCD56A3...	n/a	955BEE67763C30C...	8A3D2E168DD894...	2DB75A6FE9D35FA...
Cave size (bytes)	0x00000000 (0)	0x00000000 (0)	0x00000000 (0)	0x00000000 (0)	0x00000000 (0)
Obfuscated	-	-	-	-	-
Blacklisted	-	-	-	-	-
Read	x	x	x	x	x
Write	-	x	x	x	x
Execute	x	-	-	-	-
Shared	-	-	-	-	-

Library (7)	Blacklisted ...	Bound (0)	Type	Imported Sym...	Description
wsock32.dll	x	-	Implicit	23	Windows Socket 32-Bit DLL
winmm.dll	x	-	Implicit	1	MCI API DLL
shell32.dll	-	-	Implicit	1	Windows Shell Common Dll
kernel32.dll	-	-	Implicit	46	Windows NT BASE API Client DLL
user32.dll	-	-	Implicit	9	Multi-User Windows USER API Client DLL
advapi32.dll	-	-	Implicit	7	Advanced Windows 32 Base API
crt.dll	-	-	Implicit	23	Microsoft C Runtime Library

What functionality do these libraries potentially give the code?



NTNU

File Help



Symbol (110)	Blacklisted ...	Elevated (1)	Undocumente...	Ordinal (0)	Deprecated...	Anti-Debug...	Library (7)
WSACleanup	x	-	-	-	-	-	wsock32.dll
WSAGetLastError	x	-	-	-	-	-	wsock32.dll
WSAStartup	x	-	-	-	-	-	wsock32.dll
__WSAFDIsSet	x	-	-	-	-	-	wsock32.dll
accept	x	-	-	-	-	-	wsock32.dll
bind	x	-	-	-	-	-	wsock32.dll
closesocket	x	-	-	-	-	-	wsock32.dll
connect	x	-	-	-	-	-	wsock32.dll
gethostbyaddr	x	-	-	-	-	-	wsock32.dll
gethostbyname	x	-	-	-	-	-	wsock32.dll
getpeername	x	-	-	-	-	-	wsock32.dll
getsockname	x	-	-	-	-	-	wsock32.dll
htonl	x	-	-	-	-	-	wsock32.dll
htons	x	-	-	-	-	-	wsock32.dll
inet_addr	x	-	-	-	-	-	wsock32.dll
inet_ntoa	x	-	-	-	-	-	wsock32.dll
ioctlsocket	x	-	-	-	-	-	wsock32.dll
listen	x	-	-	-	-	-	wsock32.dll
ntohs	x	-	-	-	-	-	wsock32.dll
recv	x	-	-	-	-	-	wsock32.dll
select	x	-	-	-	-	-	wsock32.dll
send	x	-	-	-	-	-	wsock32.dll
socket	x	-	-	-	-	-	wsock32.dll
ShellExecuteA	x	-	-	-	-	-	shell32.dll
mcisendstringA	x	-	-	-	-	-	winmm.dll
ExitProcess	x	-	-	-	-	-	kernel32.dll
FindClose	x	-	-	-	-	-	kernel32.dll
FindFirstFileA	x	-	-	-	-	-	kernel32.dll
FindNextFileA	x	-	-	-	-	-	kernel32.dll
FreeLibrary	x	-	-	-	-	-	kernel32.dll
GetCommandLin...	x	-	-	-	-	-	kernel32.dll
GetCurrentProcess	x	-	-	-	-	-	kernel32.dll
GetExitCodeProc...	x	-	-	-	-	-	kernel32.dll
GetFileAttributesA	x	-	-	-	-	-	kernel32.dll
GetModuleFileN...	x	-	-	-	-	-	kernel32.dll
GetModuleHand...	x	-	-	-	-	-	kernel32.dll
GetProcAddress	x	-	-	-	-	-	kernel32.dll
GetSystemDirect...	x	-	-	-	-	-	kernel32.dll

What mischief can these
- Functions do?



NTNU

File	Help	Symbol (110)	Blacklisted ...	Elevated (1)	Undocumente...	Ordinal (0)	Deprecated...	Anti-Debug...	Library (7)
c:\users\rem\desktop\spybot.exe									
Indicators (13/21)									
Virustotal (lookup failed)									
DOS Stub (64 bytes)									
DOS Header (64 bytes)									
File Header (20 bytes)									
Optional Header (224 bytes)									
Directories (2/15)									
Sections (5)									
Imported Libraries (2/7)									
Imported Symbols (72/110)									
Exported Symbols (0)									
Exceptions (0)									
Relocations (0)									
Certificates (0)									
Thread Local Storage (n/a)									
Resources (3)									
Strings (3/247)									
Debug (n/a)									
Manifest (n/a)									
Version (1/12)									
Overlay (Unknown)									
		GetFileAttributesA	x	-	-	-	-	-	kernel32.dll
		GetModuleFileN...	x	-	-	-	-	-	kernel32.dll
		GetModuleHand...	x	-	-	-	-	-	kernel32.dll
		GetProcAddress	x	-	-	-	-	-	kernel32.dll
		GetSystemDirect...	x	-	-	-	-	-	kernel32.dll
		GetTickCount	x	-	-	-	-	x	kernel32.dll
		GetVersionExA	x	-	-	-	-	-	kernel32.dll
		GetWindowsDire...	x	-	-	-	-	-	kernel32.dll
		GlobalMemorySt...	x	-	-	-	x	-	kernel32.dll
		CopyFileA	x	-	-	-	-	-	kernel32.dll
		LoadLibraryA	x	-	-	-	-	-	kernel32.dll
		CreateDirectoryA	x	-	-	-	-	-	kernel32.dll
		MoveFileA	x	-	-	-	-	-	kernel32.dll
		OpenProcess	x	-	-	-	-	-	kernel32.dll
		PeekNamedPipe	x	-	-	-	-	-	kernel32.dll
		CreateFileA	x	-	-	-	-	-	kernel32.dll
		SetFileAttributesA	x	-	-	-	-	-	kernel32.dll
		CreateMutexA	x	-	-	-	-	-	kernel32.dll
		Sleep	x	-	-	-	-	-	kernel32.dll
		TerminateProcess	x	-	-	-	-	x	kernel32.dll
		TerminateThread	x	-	-	-	-	-	kernel32.dll
		CreatePipe	x	-	-	-	-	-	kernel32.dll
		CreateProcessA	x	-	-	-	-	-	kernel32.dll
		WriteFile	x	-	-	-	-	-	kernel32.dll
		CreateThread	x	-	-	-	-	-	kernel32.dll
		DeleteFileA	x	-	-	-	-	-	kernel32.dll
		DuplicateHandle	x	-	-	-	-	-	kernel32.dll
		GetForeground...	x	-	-	-	-	-	user32.dll
		GetKeyState	x	-	-	-	-	-	user32.dll
		GetAsyncKeyState	x	-	-	-	-	-	user32.dll
		MapVirtualKeyA	x	-	-	-	-	-	user32.dll
		ExitWindowsEx	x	x	-	-	-	-	user32.dll
		keybd_event	x	-	-	-	x	-	user32.dll
		GetUserNameA	x	-	-	-	-	-	advapi32.dll
		RegCreateKeyA	x	-	-	-	x	-	advapi32.dll
		RegCreateKeyExA	x	-	-	-	-	-	advapi32.dll
		RegOpenKeyA	x	-	-	-	x	-	advapi32.dll
		RegSetValueExA	x	-	-	-	-	-	advapi32.dll

What mischief can these Functions do?



NTNU

File	Symbol (110)	Blacklisted ...	Elevated (1)	Undocumente...	Ordinal (0)	Deprecated...	Anti-Debug...	Library (7)
c:\users\rem\desktop\spybot.exe	MapVirtualKeyA	x	-	-	-	-	-	user32.dll
Indicators (13/21)	ExitWindowsEx	x	x	-	-	-	-	user32.dll
Virustotal (lookup failed)	keybd_event	x	-	-	-	x	-	user32.dll
DOS Stub (64 bytes)	GetUserNameA	x	-	-	-	-	-	advapi32.dll
DOS Header (64 bytes)	RegCreateKeyA	x	-	-	-	x	-	advapi32.dll
File Header (20 bytes)	RegCreateKeyExA	x	-	-	-	-	-	advapi32.dll
Optional Header (224 bytes)	RegOpenKeyA	x	-	-	-	x	-	advapi32.dll
Directories (2/15)	RegSetValueExA	x	-	-	-	-	-	advapi32.dll
Sections (5)	fwrite	x	-	-	-	-	-	crt.dll
Imported Libraries (2/7)	GetDateFormatA	-	-	-	-	-	-	kernel32.dll
Imported Symbols (72/110)	GetFileSize	-	-	-	-	-	-	kernel32.dll
Exported Symbols (0)	GetLastError	-	-	-	-	-	-	kernel32.dll
Exceptions (0)	CloseHandle	-	-	-	-	-	-	kernel32.dll
Relocations (0)	GetTimeFormatA	-	-	-	-	-	-	kernel32.dll
Certificates (0)	ReadFile	-	-	-	-	-	-	kernel32.dll
Thread Local Storage (n/a)	RtlUnwind	-	-	-	-	-	-	kernel32.dll
Resources (3)	SetFilePointer	-	-	-	-	-	-	kernel32.dll
Strings (3/247)	IstrcpyA	-	-	-	-	x	-	kernel32.dll
Debug (n/a)	IstrcpynA	-	-	-	-	x	-	kernel32.dll
Manifest (n/a)	IstrlenA	-	-	-	-	x	-	kernel32.dll
Version (1/12)	GetWindowTextA	-	-	-	-	-	-	user32.dll
Overlay (Unknown)	CharUpperBuffA	-	-	-	-	-	-	user32.dll
	CharToOemA	-	-	-	-	x	-	user32.dll
	RegCloseKey	-	-	-	-	-	-	advapi32.dll
	RegQueryValueE...	-	-	-	-	-	-	advapi32.dll
	__GetMainArgs	-	-	-	-	-	-	crt.dll
	atoi	-	-	-	-	-	-	crt.dll
	exit	-	-	-	-	-	-	crt.dll
	fclose	-	-	-	-	-	-	crt.dll
	fopen	-	-	-	-	x	-	crt.dll
	fputc	-	-	-	-	-	-	crt.dll
	fputs	-	-	-	-	-	-	crt.dll
	fread	-	-	-	-	-	-	crt.dll
	malloc	-	-	-	-	-	-	crt.dll
	memcpy	-	-	-	-	x	-	crt.dll
	memset	-	-	-	-	x	-	crt.dll
	raise	-	-	-	-	-	-	crt.dll

What mischief can these Functions do?

String – What stands out?

PeStudio 8.42 - Win

File Help

c:\users\rem\desktop\spybot.exe

- Indicators (13/21)
- VirusTotal (lookup failed)
- DOS Stub (64 bytes)
- DOS Header (64 bytes)
- File Header (20 bytes)
- Optional Header (224 bytes)
- Directories (2/15)
- Sections (5)
- Imported Libraries (2/7)
- Imported Symbols (72/110)
- Exported Symbols (0)
- Exceptions (0)
- Relocations (0)
- Certificates (0)
- Thread Local Storage (n/a)
- Resources (3)
- Strings (3/247)**
- Debug (n/a)
- Manifest (n/a)
- Version (1/12)
- Overlay (Unknown)

Type	Size	Blacklisted ...	Value
ascii	11	x	wuaumgr.exe
unicode	11	x	wuaumgr.exe
unicode	11	x	wuaumgr.exe
ascii	40	-	This program cannot be run in DOS mode.
ascii	5	-	.text
ascii	5	-	.bss
ascii	5	-	.data
ascii	6	-	.idata
ascii	5	-	.rsrc
ascii	7	-	t;t\$\$t
ascii	5	-	SVWUj
ascii	4	-]_^[
ascii	4	-	SVWU
ascii	4	-	t:VU
ascii	4	-	t(x1
ascii	4	-]_^[
ascii	4	-	=, A
ascii	4	-	h(A
ascii	4	-	h\$ A
ascii	4	-	h A
ascii	4	-	5(A



Type	Size	Blacklisted ...	Value
ascii	4	-	%xDA
ascii	4	-	% DA
ascii	10	-	# - xXx -
ascii	8	-	xTriplex
ascii	14	-	Winsock driver
ascii	5	-	krnel
ascii	25	-	xXx - Triple Threat - xXx
ascii	10	-	keylog.txt
ascii	4	-	tsm~
ascii	4	-	tsm~
ascii	22	-	Error operation failed
ascii	19	-	Operation completed
unicode	46	-	?><MNBVCXZ":LKJHGFDSA){POIUYTREWQ_}(&^%\$#@!~+*
unicode	33	-]V.,mnbvcxz;lkjhgfdsa][poiuytrwq
unicode	14	-]=-0987654321`
unicode	7	-	APPICON
unicode	15	-	VS_VERSION_INFO
unicode	14	-	StringFileInfo
unicode	8	-	040904B0
unicode	11	-	CompanyName
unicode	21	-	Microsoft Corporation
unicode	15	-	FileDescription
unicode	39	-	Generic Host Process for Win32 Services
unicode	11	-	FileVersion
unicode	34	-	5.1.2700.0 (NT client.010817-1148)
unicode	12	-	InternalName
unicode	14	-	LegalCopyright
unicode	44	-	Microsoft Corporation. All rights reserved.
unicode	16	-	OriginalFilename
unicode	11	-	ProductName
unicode	9	-	Microsoft
unicode	8	-	Windows
unicode	17	-	Operating System
unicode	14	-	ProductVersion
unicode	10	-	5.1.2700.0
unicode	11	-	VarFileInfo
unicode	11	-	Translation

File Help



c:\users\rem\desktop\spybot.exe

- Indicators (13/21)
- Virustotal (lookup failed)
- DOS Stub (64 bytes)
- DOS Header (64 bytes)
- File Header (20 bytes)
- Optional Header (224 bytes)
- Directories (2/15)
- Sections (5)
- Imported Libraries (2/7)
- Imported Symbols (72/110)
- Exported Symbols (0)
- Exceptions (0)
- Relocations (0)
- Certificates (0)
- Thread Local Storage (n/a)
- Resources (3)
- Strings (3/247)
- Debug (n/a)
- Manifest (n/a)
- Version (1/12)**
- Overlay (Unknown)

Property	Value
File OS	Windows 32-bit
File Type	Executable
File Date	n/a
CompanyName	Microsoft Corporation
FileDescription	Generic Host Process for Win32 Services
FileVersion	5.1.2700.0 (NT client.010817-1148)
InternalName	wuaumgr.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	wuaumgr.exe
ProductName	Microsoft® Windows® Operating System
ProductVersion	5.1.2700.0
Translation Information	
Language	1033 (en-US)
Code page	1200

Hypothesis

- Keylogger with network capabilities. Can manipulated both files and registries. Can start new processes and threads. May have anti debug capabilities and use mutex. Look for keylog.exe, wuaumqr.exe
- Pluss loads more... with strings from V8.54

Summary

- Basic static analysis
 - Simple first step
 - Get a first impression and collect some IOC
 - Get help decide where to start deeper analysis
- Next
 - Basic dynamic analysis
 - Need a safe environment to execute malware
 - NB! Always use safe environment.