MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**asd.exe**
ID	#6594433
MD5	4d583ae773f28a6fdcd29a2aa13de118
SHA1	64cb42f87def47d5f189531b8af14bb5ba2085c0
SHA256	b030e5e7fc31e7d9f6c10101bb088df7dfcc64e78bb2da889c1253ffb3b520db
File Size	7703.00 KB
Report Created	2024-03-29 05:50 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 17 matches)

Score	Category	Operation	Count	Classification
5/5	Anti Analysis	Makes indirect system call to possibly evade hooking based monitoring	1	-
	• (Process #1) asd.exe makes an indirect system call to "NtProtectVirtualMemory".			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #1) asd.exe hides thread via API "NtSetInformationThread".			
3/5	Anti Analysis	Modifies native system functions	1	-
	• (Process #1) asd.exe modifies native system functions, possibly to evade hooking.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #1) asd.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #1) asd.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) asd.exe tries to detect "Sandboxie" by checking for existence of module "sbiedll.dll".			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) asd.exe is possibly trying to detect a VM via rdtsc.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based monitoring	10	-
	• (Process #1) asd.exe makes a direct system call to "NtQuerySystemInformation". • (Process #1) asd.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #1) asd.exe makes a direct system call to "NtQueryVirtualMemory". • (Process #1) asd.exe makes a direct system call to "NtClose". • (Process #1) asd.exe makes a direct system call to "NtOpenFile". • (Process #1) asd.exe makes a direct system call to "NtMapViewOfSection". • (Process #1) asd.exe makes a direct system call to "NtCreateSection". • (Process #1) asd.exe makes a direct system call to "NtQueryInformationProcess". • (Process #1) asd.exe makes a direct system call to "NtProtectVirtualMemory". • (Process #1) asd.exe makes a direct system call to "NtSetInformationThread".			

Mitre ATT&CK Matrix

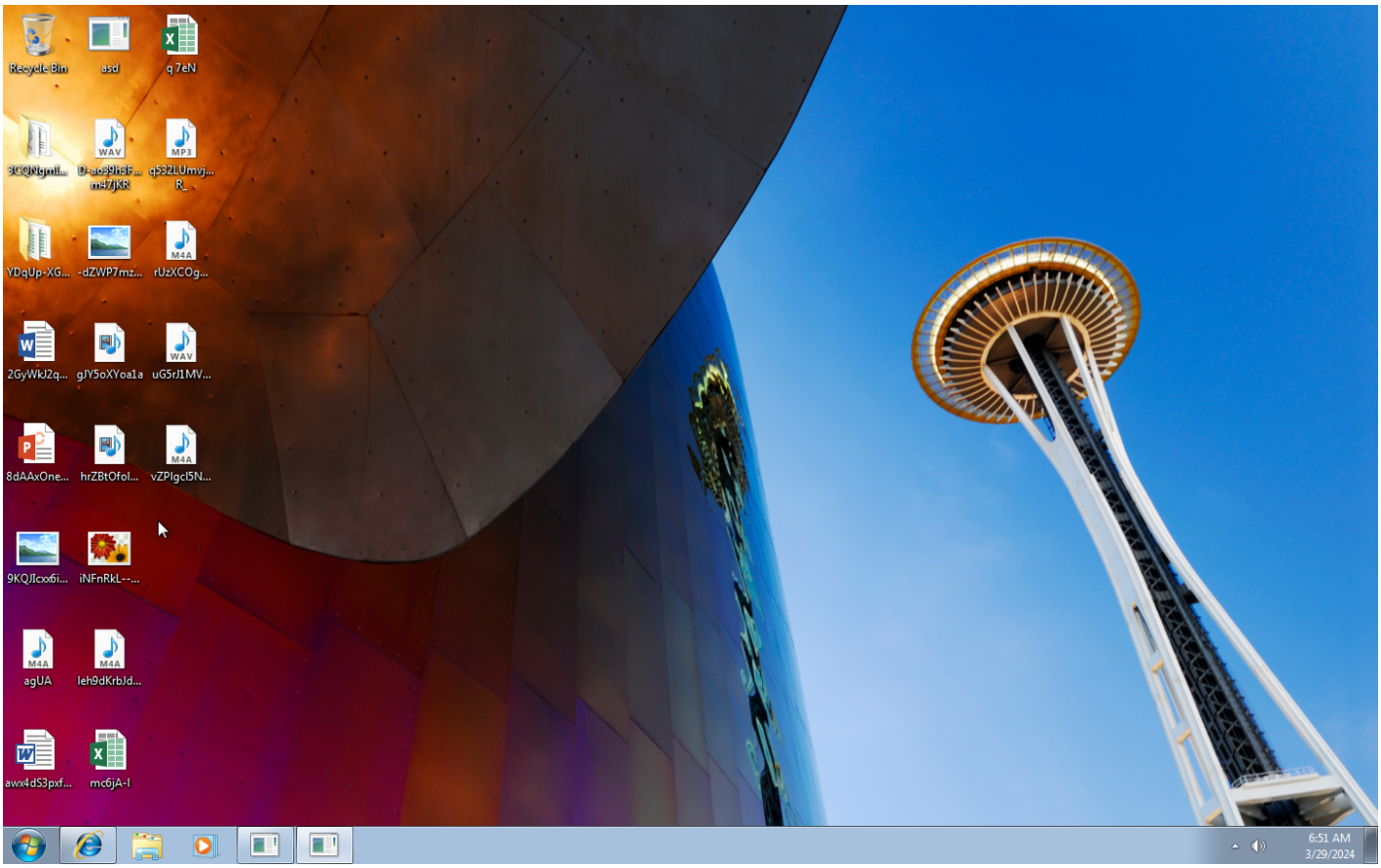
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					

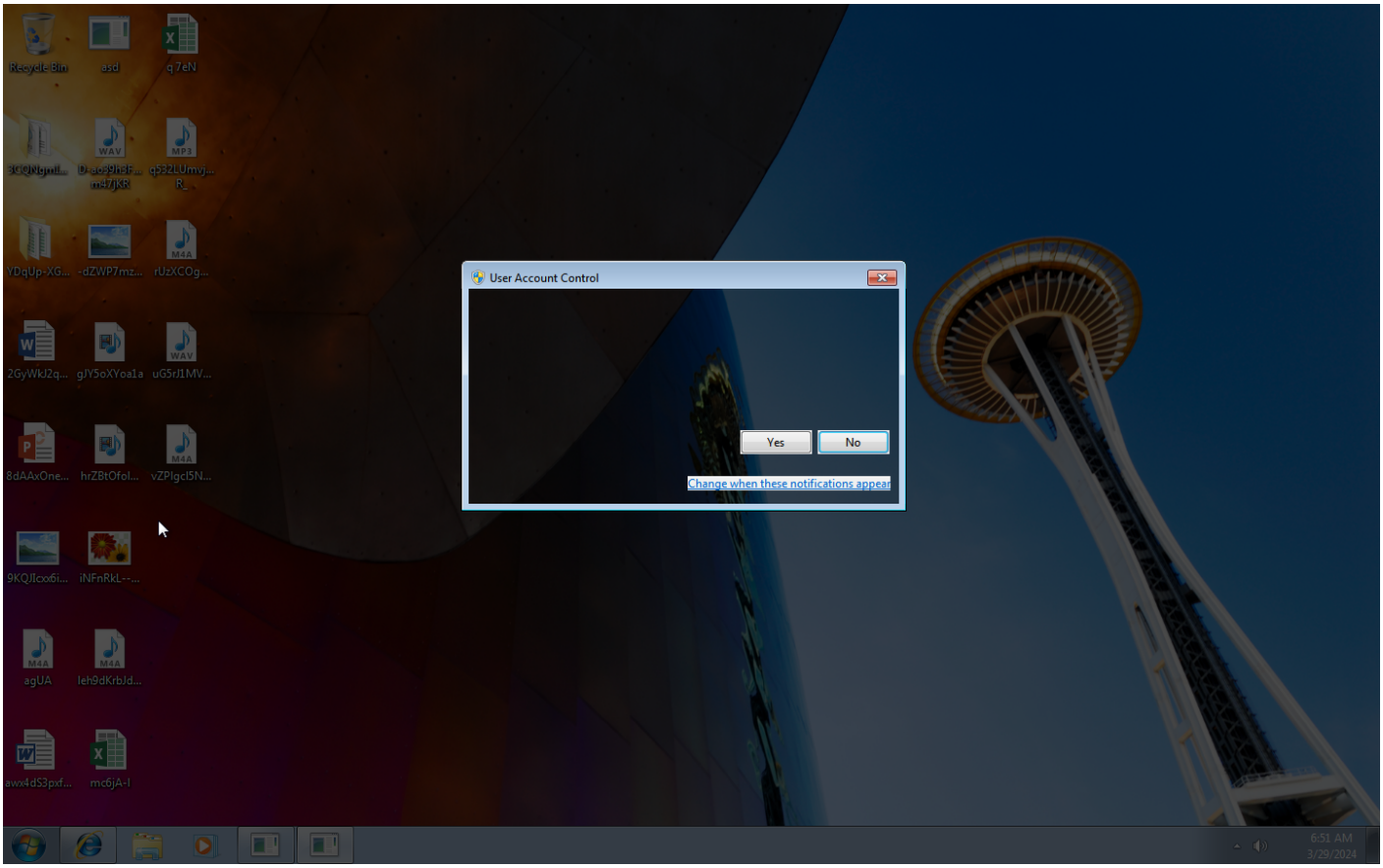
Sample Information

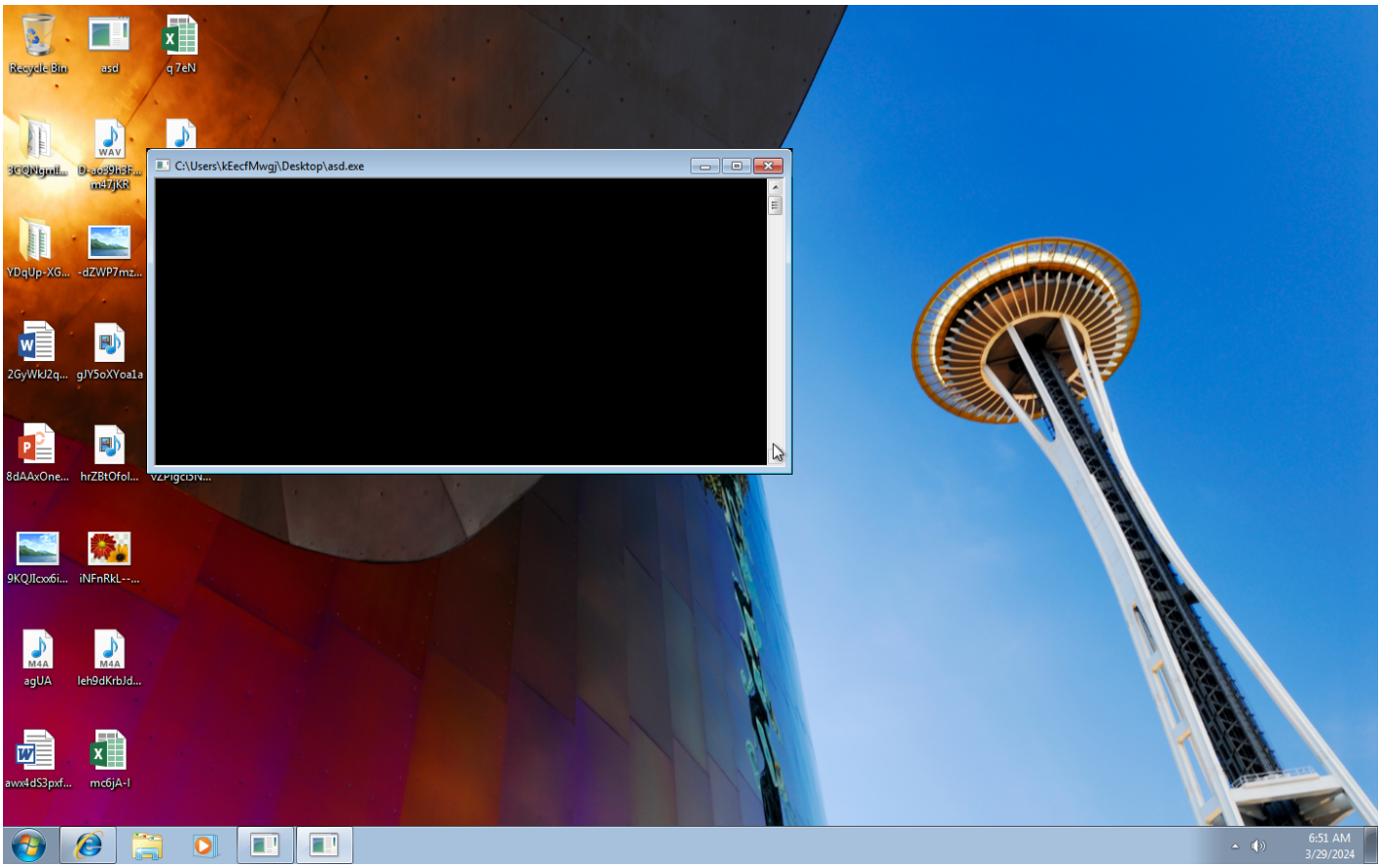
ID	#6594433
MD5	4d583ae773f28a6fdcd29a2aa13de118
SHA1	64cb42f87def47d5f189531b8af14bb5ba2085c0
SHA256	b030e5e7fc31e7d9f6c10101bb088df7dfcc64e78bb2da889c1253ffb3b520db
SSDeep	196608:mJB7BuVHvQBaUdlNboLE6utxn+WlaMUDijGnSNTFgV9eA:mEVHMObuU+WlaMRGnUK
ImpHash	7b529fd349f98535301bf9c7230b0b1d
File Name	asd.exe
File Size	7703.00 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

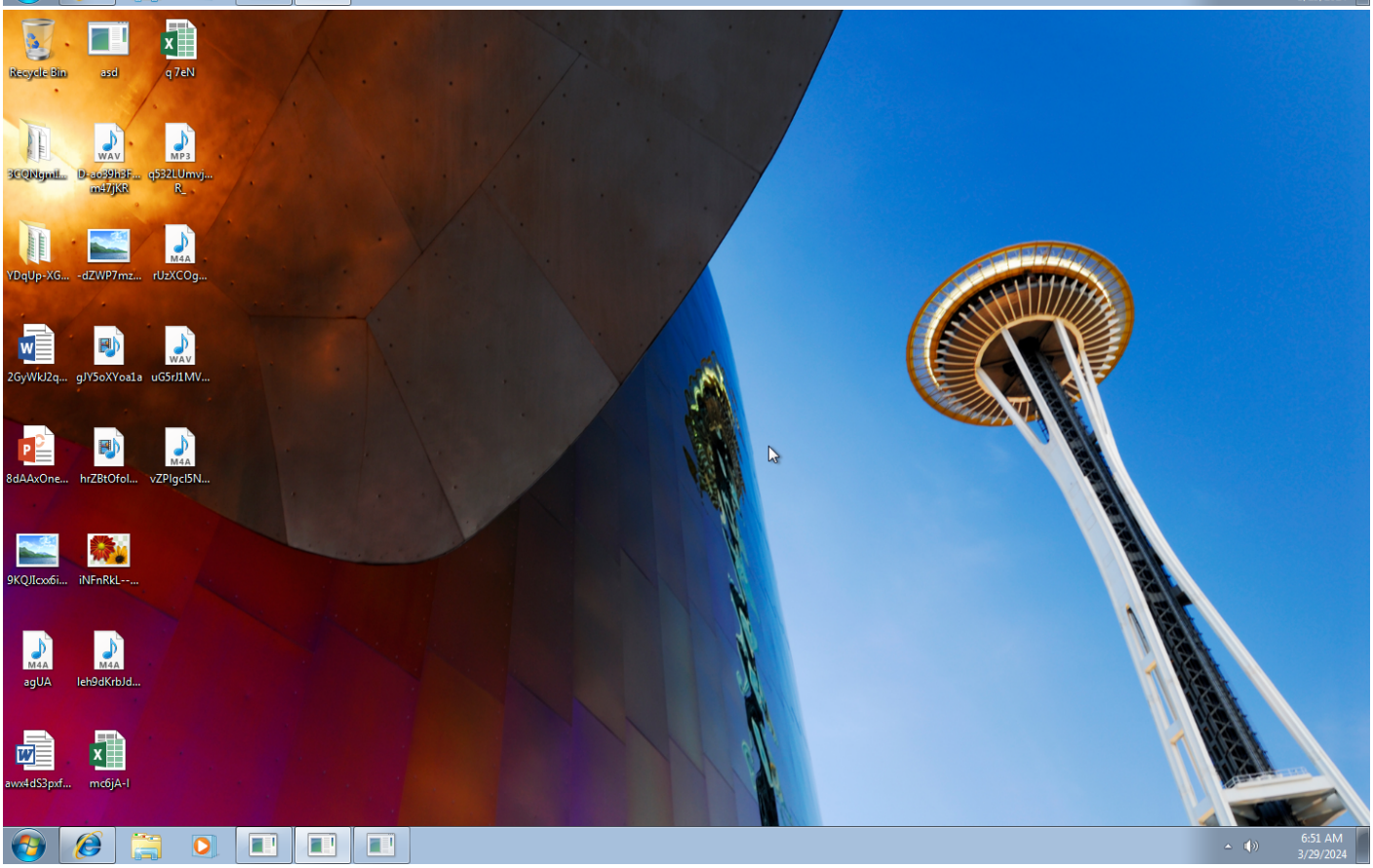
Analysis Information

Creation Time	2024-03-29 05:50 (UTC)
Analysis Duration	00:00:16
Termination Reason	All processes terminated
Number of Monitored Processes	1
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✖
Built-in AV Enabled	✔
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
asd
q 7eN
6:51 AM
3/29/2024


Recycle Bin
asd
q 7eN
User Account Control
Yes
No
Change when these notifications appear
6:51 AM
3/29/2024


Recycle Bin
asd
q 7eN
C:\Users\kEecfMwgj\Desktop\asd.exe
6:51 AM
3/29/2024


Recycle Bin
asd
q 7eN
6:51 AM
3/29/2024

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

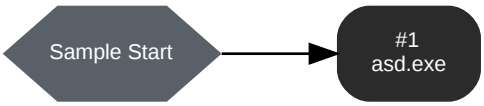
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: asd.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\asd.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\asd.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45633, Reason: Analysis Target
Unmonitor End Time	End Time: 51472, Reason: Terminated
Monitor duration	5.84s
Return Code	3
PID	3656
Parent PID	-
Bitness	64 Bit

Host Behavior

Type	Count
-	8
-	1
System	23
File	13
Module	37
Process	1
Environment	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b030e5e7fc31e7d9f6c10101bb088df7dfcc64e78bb2da889c1253ffb3b520db	C:\Users\kEecfMwgj\Desktop\asd.exe	Sample File	7703.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\asd.exe	Accessed File, Sample File	Access	MALICIOUS
\??\C:\Users\kEecfMwgj\Desktop\asd.exe	Accessed File	Access	CLEAN

Process

Process Name	Commandline	Verdict
asd.exe	"C:\Users\kEecfMwgj\Desktop\asd.exe"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	windows 7 (64bit SP1 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.9 / 2024-03-26 09:11:11
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.5 / 2024-03-22 20:39:30
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.12 / 2024-03-28 09:41:51
YARA Built-in Ruleset Version	2024.2.1.11

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.21 (August 15, 2021)
Built-in AV Database Update Release Date	2024-03-29 01:11:30
Built-in AV Database Records	13869638

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop

Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows