MALICIOUS

Classifications: Spyware

Threat Names: Agent Tesla v3, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe**
ID	#967593
MD5	81b92680fb33ddfaccae09031e1888f2
SHA1	880a7e88ca219c5361ddfbad786bfeea9bb6b6fa
SHA256	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac
File Size	720.50 KB
Report Created	2021-09-27 23:15 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 29 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe".			
4/5	System Modification	Modifies network configuration	1	-
	• (Process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe modifies the host.conf file, probably to redirect network traffic.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	2	-
	• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe modifies memory of (process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe. • (Process #9) kpruegc.exe modifies memory of (process #13) kpruegc.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	2	-
	• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe alters context of (process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe. • (Process #9) kpruegc.exe alters context of (process #13) kpruegc.exe.			
1/5	Mutex	Creates mutex	2	-
	• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe creates mutex with name "mLNPTFHTEO". • (Process #9) kpruegc.exe creates mutex with name "mLNPTFHTEO".			
1/5	Privilege Escalation	Enables process privilege	4	-
	• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe enables process privilege "SeDebugPrivilege". • (Process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe enables process privilege "SeDebugPrivilege". • (Process #9) kpruegc.exe enables process privilege "SeDebugPrivilege". • (Process #13) kpruegc.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe starts (process #2) schtasks.exe with a hidden window. • (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe starts (process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe with a hidden window. • (Process #9) kpruegc.exe starts (process #12) schtasks.exe with a hidden window. • (Process #9) kpruegc.exe starts (process #13) kpruegc.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	2	-

Score	Category	Operation	Count	Classification
		• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe reads from (process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe. • (Process #9) kpruegc.exe reads from (process #13) kpruegc.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	2	-
		• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #9) kpruegc.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Persistence	Installs system startup script or application	1	-
		• (Process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe" to Windows startup via registry.		
1/5	System Modification	Modifies operating system directory	1	-
		• (Process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe creates file "C:\Windows\system32\drivers\etc\hosts" in the OS directory.		
1/5	Execution	Executes itself	2	-
		• (Process #1) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe. • (Process #9) kpruegc.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe.		
1/5	Obfuscation	Resolves API functions dynamically	2	-
		• (Process #3) ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe resolves 50 API functions by name. • (Process #13) kpruegc.exe resolves 50 API functions by name.		

Mitre ATT&CK Matrix

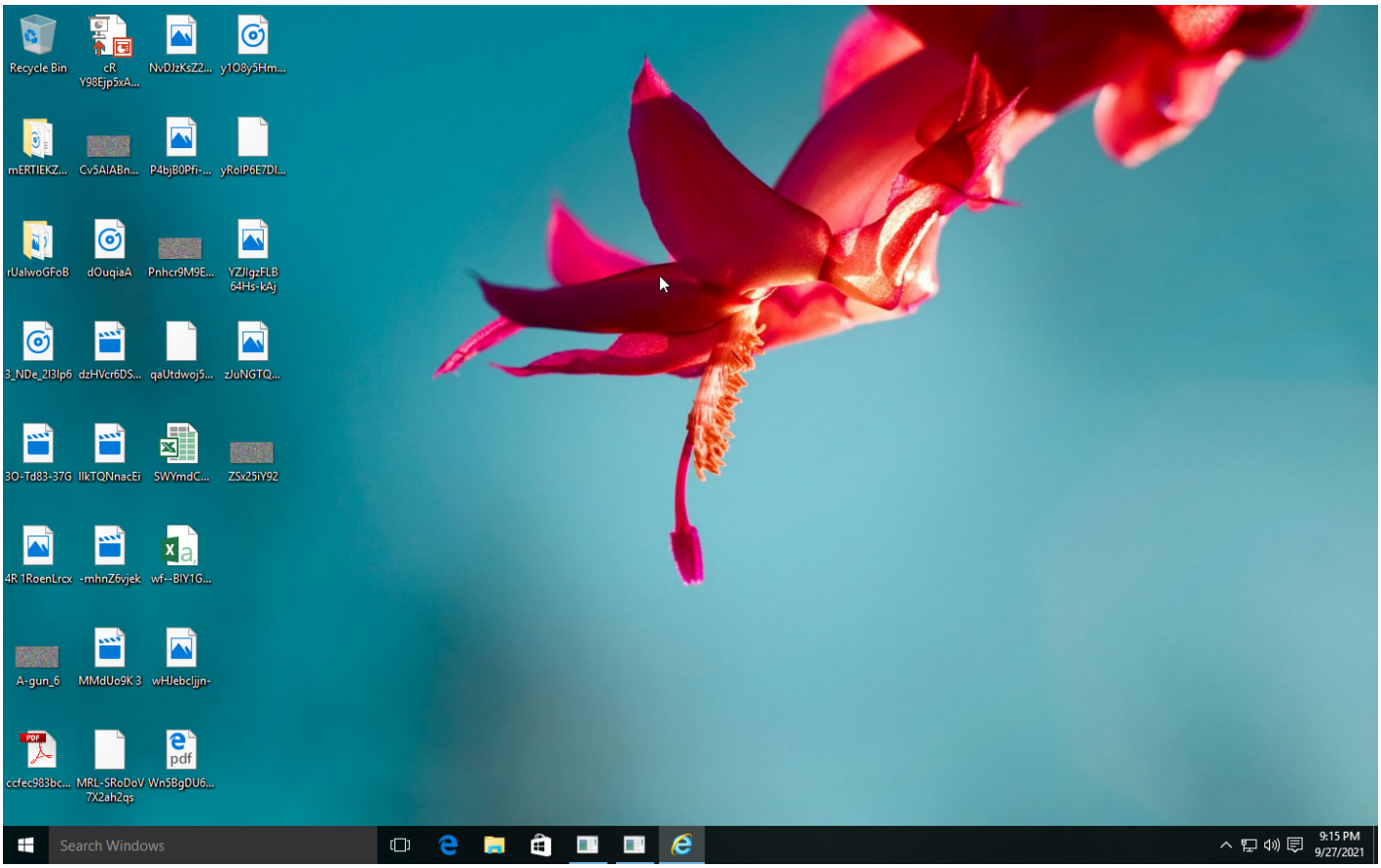
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window		#T1497 Virtualization/ Sandbox Evasion			#T1090 Connection Proxy		
				#T1045 Software Packing		#T1124 System Time Discovery					
				#T1112 Modify Registry							
				#T1096 NTFS File Attributes							
				#T1497 Virtualization/ Sandbox Evasion							

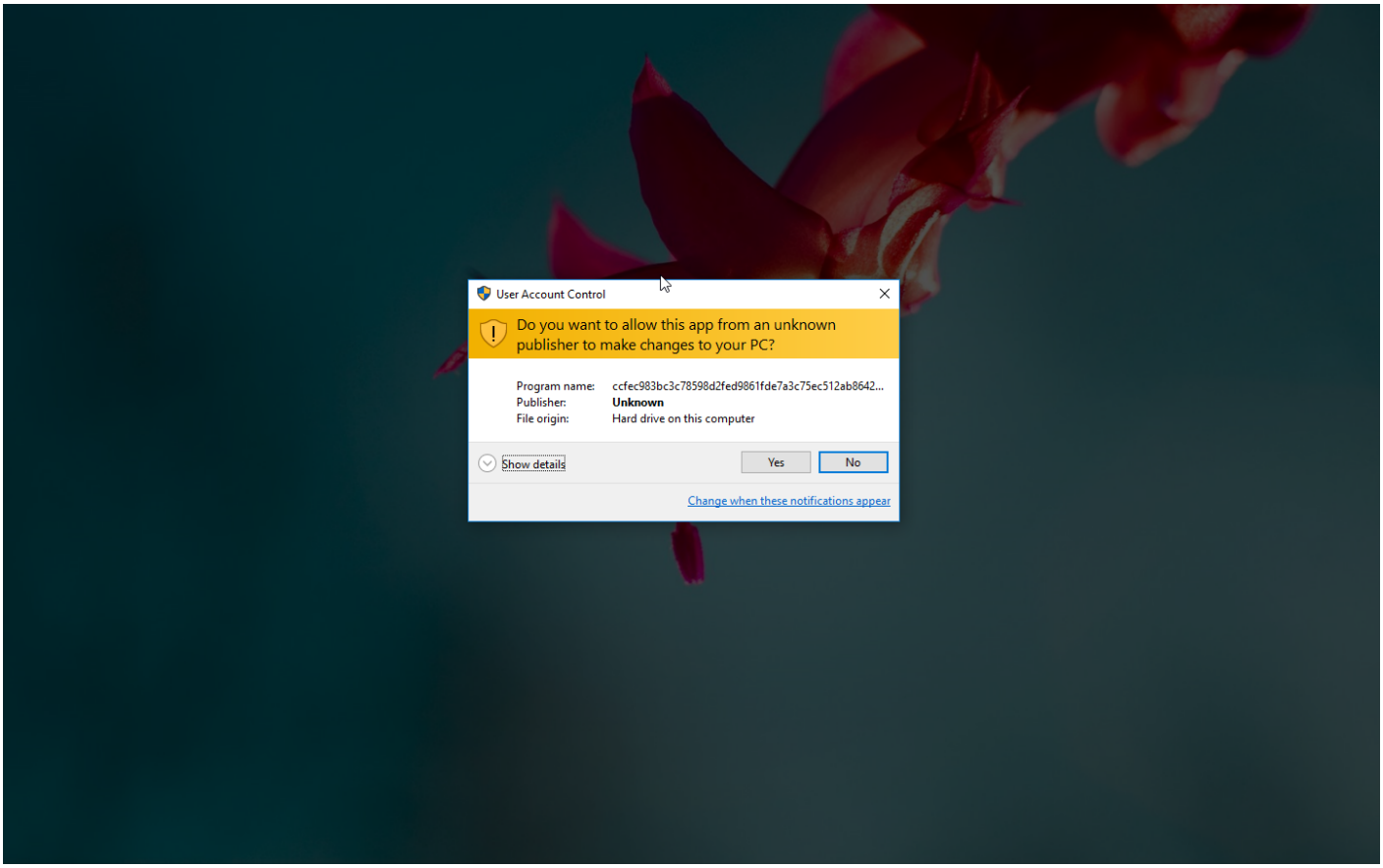
Sample Information

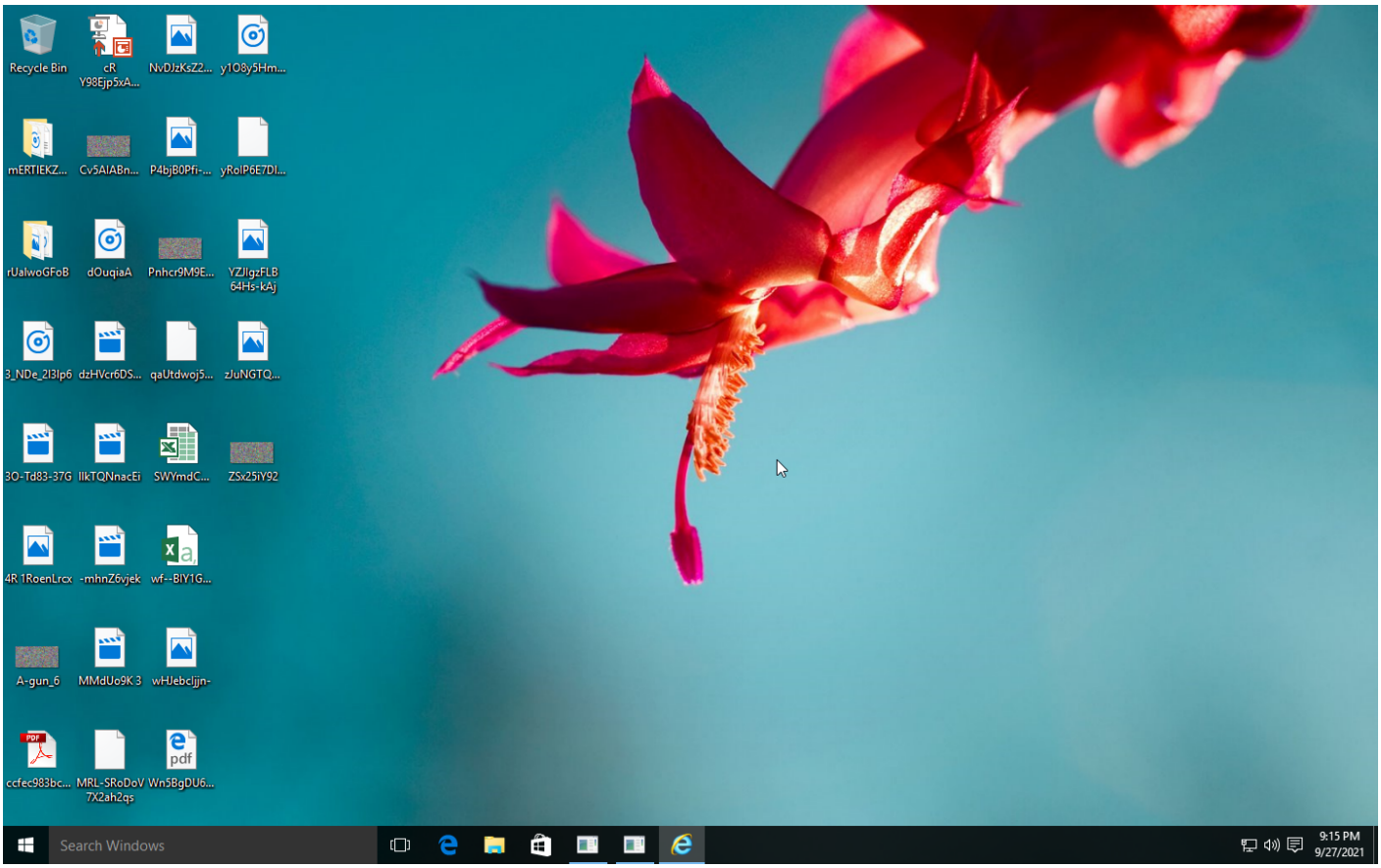
ID	#967593
MD5	81b92680fb33ddfaccae09031e1888f2
SHA1	880a7e88ca219c5361ddfbad786bfeea9bb6b6fa
SHA256	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac
SSDeep	12288:juZqIF/OXft1u0J9mmbXQBy79MxXhWnTl+uXk56gpmz7zLmMr52HEAmD:AqIFm/u0Xmk2y7UXsTg6QgHC
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe
File Size	720.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

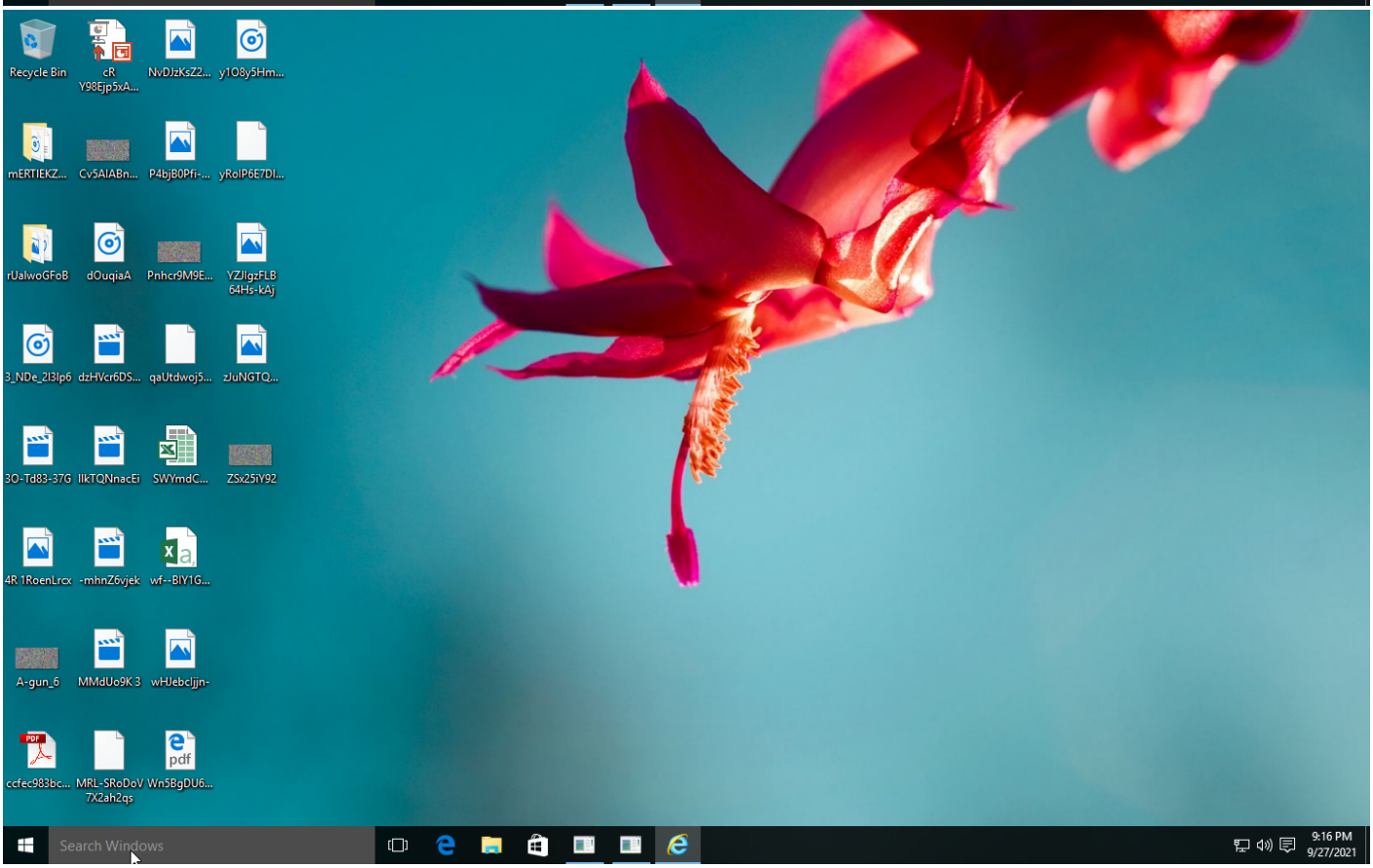
Analysis Information

Creation Time	2021-09-27 23:15 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
Execution Successful	False
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	1


Recycle Bin
cR Y98Ejp5xA...
NvDJzKsZ2...
y1O8y5Hm...
mERTIEKZ...
Cv5AIABn...
P4bjB0Pfi-...
yRolP6E7DI...
rUaIwoGFoB
dOuqiaA
Pnhcr9M9E...
YZJlgzFLB 64Hs-kAj
3_NDe_2l3lp6
dzHVcr6DS...
qaUtdwoj5...
zJuNGTQ...
3O-Td83-37G
IlkTQNnacEi
SWYmdC...
ZSx25iY92
4R 1RoenLrcx
-mhnZ6vjek
wf--BIY1G...
A-gun_6
MMdUo9K 3
wHJebcljjn-
ccfec983bc...
MRL-SRoDoV 7X2ah2qs
Wn5BgDU6...
Search Windows
9:15 PM
9/27/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

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

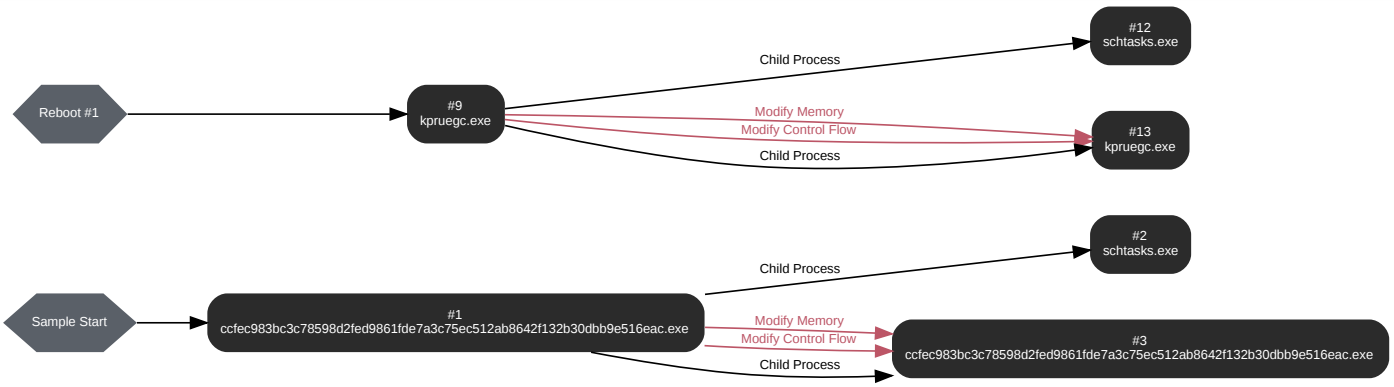
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 46158, Reason: Analysis Target
Unmonitor End Time	End Time: 116442, Reason: Terminated
Monitor duration	70.28s
Return Code	0
PID	2820
Parent PID	1636
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\xlpVvRzhctudF.exe	720.50 KB	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp43D6.tmp	1.61 KB	0c85484f8b21e89e70f588eaff182bfd0cfef5df63832a3249728fb7c247a69b	✗

Host Behavior

Type	Count
Module	47
System	6
Window	6
Registry	3
File	10
Mutex	2
User	2
Process	2
-	3
-	7

Process #2: schtasks.exe

ID	2
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xIpVvRzhctudF" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp43D6.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113839, Reason: Child Process
Unmonitor End Time	End Time: 125646, Reason: Terminated
Monitor duration	11.81s
Return Code	1
PID	2016
Parent PID	2820
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	13

Process #3: ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 114345, Reason: Child Process
Unmonitor End Time	End Time: 176818, Reason: Terminated
Monitor duration	62.47s
Return Code	1073807364
PID	2256
Parent PID	2820
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	0x484	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	0x484	0x402000(4202496)	0x35c00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	0x484	0x438000(4423680)	0x600	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	0x484	0x43a000(4431872)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	0x484	0x2c5008(2904072)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	0x484 / 0xd10		-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe	720.50 KB	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac	✗

Host Behavior

Type	Count
Module	59
Window	3
System	14
Registry	28

Type	Count
User	2
-	15
File	34
COM	24
Environment	3

Process #9: kpruegc.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 233808, Reason: Autostart
Unmonitor End Time	End Time: 274135, Reason: Terminated
Monitor duration	40.33s
Return Code	0
PID	3344
Parent PID	1556
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp433E.tmp	1.61 KB	0c85484f8b21e89e70f588eaff182bfd0cfef5df63832a3249728fb7c247a69b	✗

Host Behavior

Type	Count
Module	47
System	2
Window	6
Registry	3
File	8
Mutex	2
User	1
Process	2
-	3
-	7

Process #12: schtasks.exe

ID	12
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xIpVvRzhctudF" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp433E.tmp"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 272070, Reason: Child Process
Unmonitor End Time	End Time: 274626, Reason: Terminated
Monitor duration	2.56s
Return Code	1
PID	3744
Parent PID	3344
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	13

Process #13: kpruegc.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 272180, Reason: Child Process
Unmonitor End Time	End Time: 286264, Reason: Terminated by Timeout
Monitor duration	14.08s
Return Code	Unknown
PID	3752
Parent PID	3344
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe	0xd14	0x400000(4194304)	0x200	✓	1
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe	0xd14	0x402000(4202496)	0x35c00	✓	1
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe	0xd14	0x438000(4423680)	0x600	✓	1
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe	0xd14	0x43a000(4431872)	0x200	✓	1
Modify Memory	#9: c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe	0xd14	0x30a008(3186696)	0x4	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\appdata\roaming\kpruegc\kpruegc.exe	0xd14 / 0xeac		-	✓	1

Host Behavior

Type	Count
Module	56
Window	3
System	4
Registry	14
User	1
-	7
File	19
COM	12

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac	C:\Users\RDhJ0CNFevzX\AppData\Roaming\xlpVvRzhctudF.exe, C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe	Sample File	720.50 KB	application/vnd.microsoft.portable-executable	Create, Access, Write	MALICIOUS
9b13a3ea948a1071a81787aac1930b89e30df22ce13f8ff751f31b5d83e79ffb	C:\Windows\system32\drivers\etc\hosts	Modified File	835 bytes	text/plain	Create, Access, Write	CLEAN
0c85484f8b21e89e70f588eaff182bfd0cfef5df63832a3249728fb7c247a69b	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp433E.tmp, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp43D6.tmp	Dropped File	1.61 KB	text/xml	Create, Delete, Access, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\xlpVvRzhctudF.exe	Sample File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp43D6.tmp	Dropped File	Create, Delete, Access, Write	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe	Sample File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Windows\system32\drivers\etc\hosts	Modified File	Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp433E.tmp	Dropped File	Create, Delete, Access, Write	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
mLNPTFHTEO	access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	kpruegc.exe, ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\kprUEGC	read, access, write	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	CLEAN

Process

Process Name	Commandline	Verdict
ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	"C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe"	MALICIOUS

Process Name	Commandline	Verdict
ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe	"C:\Users\RDhJ0CNFevzX\Desktop\ccfec983bc3c78598d2fed9861fde7a3c75ec512ab8642f132b30dbb9e516eac.exe"	MALICIOUS
kpruegc.exe	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe"	MALICIOUS
kpruegc.exe	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\kprUEGC\kprUEGC.exe"	SUSPICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xlpVvRzhctudF" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp43D6.tmp"	CLEAN
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xlpVvRzhctudF" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp433E.tmp"	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-27 18:53:08+00:00
Built-in AV Database Records	10474020

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows