MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**2a29d10ec3310613657d8a0dcaa4aabe.virus.exe**
ID	#10314539
MD5	2a29d10ec3310613657d8a0dcaa4aabe
SHA1	f99a7d5d2ce42d5bb5ddc4c66db6ed7eb8d9bb58
SHA256	05b8805d514836fe3de91c1a34ba61a97c9c9ab46f380b65f81ab26cb1cb63d5
File Size	20745.32 KB
Report Created	2024-04-27 09:25 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 48 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #5) avscan.exe modifies the content of multiple user files.			
4/5	Masquerade	Masks file extension	1	-
	• The executable file C:\Users\kEecfMwgj\Desktop\A0jRdmcvV1haBm5.doc has a Word document extension.			
4/5	Reputation	Malicious file detected via reputation	2	-
	• Reputation analysis labels file "c:\windows\W_X_C.bat" as Mal/Generic-S. • Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe hides thread via API "NtSetInformationThread".			
2/5	Discovery	Searches for sensitive browser data	4	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #5) avscan.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #9) avscan.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #11) hosts.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Execution	Sends control codes to a driver	4	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe controls driver "\\.\C:" through API DeviceIOControl. • (Process #5) avscan.exe controls driver "\\.\C:" through API DeviceIOControl. • (Process #9) avscan.exe controls driver "\\.\C:" through API DeviceIOControl. • (Process #11) hosts.exe controls driver "\\.\C:" through API DeviceIOControl.			
2/5	Anti Analysis	Delays execution	2	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe has a thread which sleeps more than 5 minutes. • (Process #5) avscan.exe has a thread which sleeps more than 5 minutes.			
1/5	Defense Evasion	Accesses volumes directly	4	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe opens a handle to directly access the volume "C". • (Process #5) avscan.exe opens a handle to directly access the volume "C". • (Process #9) avscan.exe opens a handle to directly access the volume "C". • (Process #11) hosts.exe opens a handle to directly access the volume "C".			
1/5	System Modification	Modifies operating system directory	5	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe creates file "C:\windows\W_X_C.vbs" in the OS directory. • (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe creates file "c:\windows\W_X_C.bat" in the OS directory. • (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe creates file "C:\Windows\hosts.exe" in the OS directory. • (Process #5) avscan.exe modifies file "C:\Windows\hosts.exe" in the OS directory. • (Process #11) hosts.exe modifies file "C:\Windows\hosts.exe" in the OS directory.			
1/5	Persistence	Installs system startup script or application	4	-

Score	Category	Operation	Count	Classification
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe adds "C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe" to Windows startup via registry. • (Process #8) wscript.exe adds "W_X_C.bat" to Windows startup via registry. • (Process #5) avscan.exe adds "C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe" to Windows startup via registry. • (Process #13) wscript.exe adds "W_X_C.bat" to Windows startup via registry.			
1/5	Hide Tracks	Creates process with hidden window	7	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe starts (process #2) reg.exe with a hidden window. • (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe starts (process #5) avscan.exe with a hidden window. • (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe starts (process #6) cmd.exe with a hidden window. • (Process #5) avscan.exe starts (process #9) avscan.exe with a hidden window. • (Process #5) avscan.exe starts (process #10) cmd.exe with a hidden window. • (Process #5) avscan.exe starts (process #12) reg.exe with a hidden window. • (Process #11) hosts.exe starts (process #14) avscan.exe with a hidden window.			
1/5	Obfuscation	Resolves API functions dynamically	5	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe resolves 503 API functions by name. • (Process #5) avscan.exe resolves 474 API functions by name. • (Process #9) avscan.exe resolves 253 API functions by name. • (Process #11) hosts.exe resolves 250 API functions by name. • (Process #14) avscan.exe resolves 151 API functions by name.			
1/5	Obfuscation	Overwrites code	4	-
	• (Process #9) avscan.exe overwrites code to possibly hide behavior. • (Process #11) hosts.exe overwrites code to possibly hide behavior. • (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe overwrites code to possibly hide behavior. • (Process #5) avscan.exe overwrites code to possibly hide behavior.			
1/5	Execution	Drops PE file	2	-
	• (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe drops file "C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe". • (Process #1) 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe drops file "C:\Windows\hosts.exe".			
1/5	Crash	A monitored process crashed	1	-
	• (Process #7) hosts.exe crashed.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe".			

Mitre ATT&CK Matrix

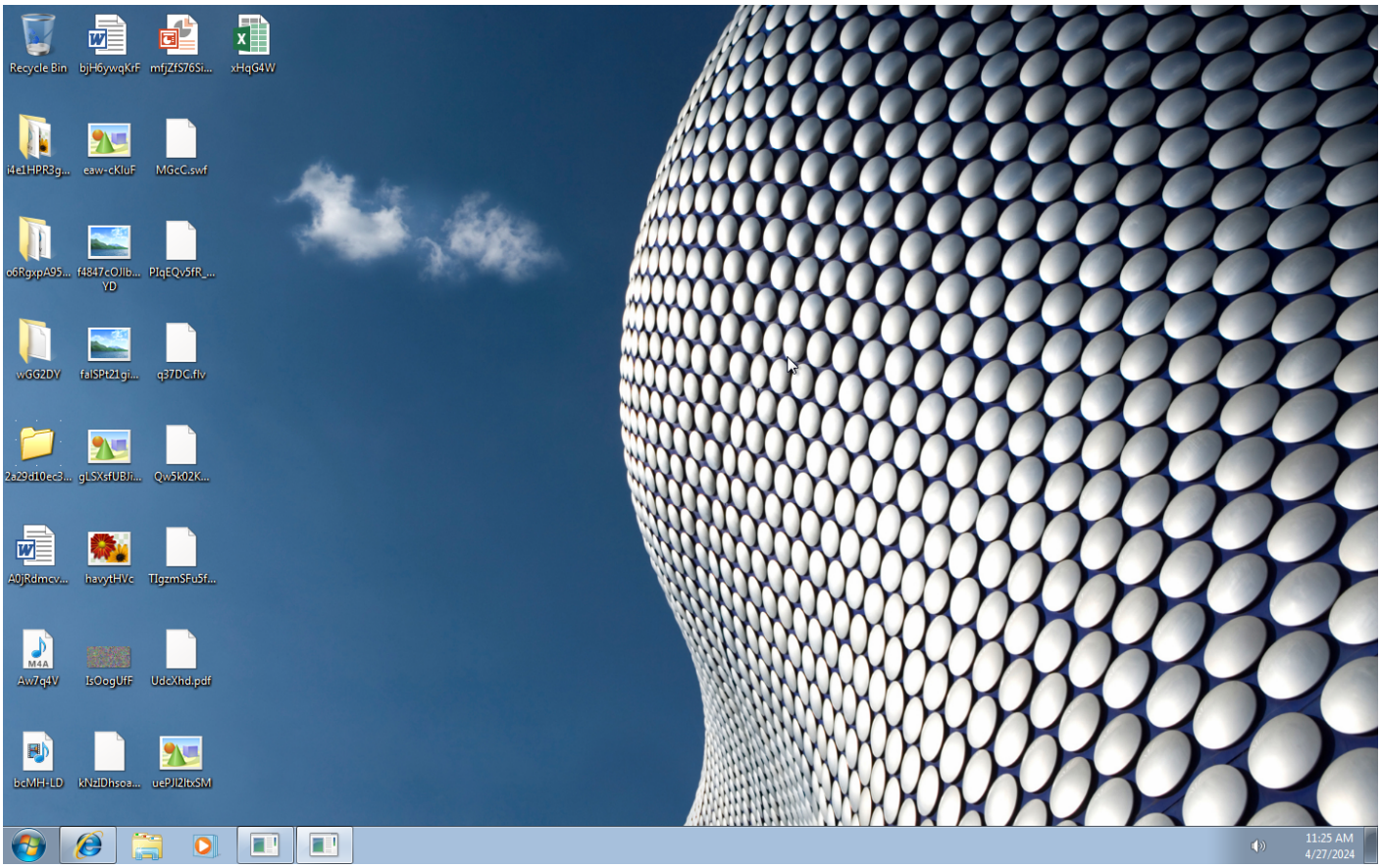
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1006 File System Logical Offsets	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
				#T1112 Modify Registry				#T1005 Data from Local System			
				#T1143 Hidden Window							
				#T1036 Masquerading							
				#T1045 Software Packing							

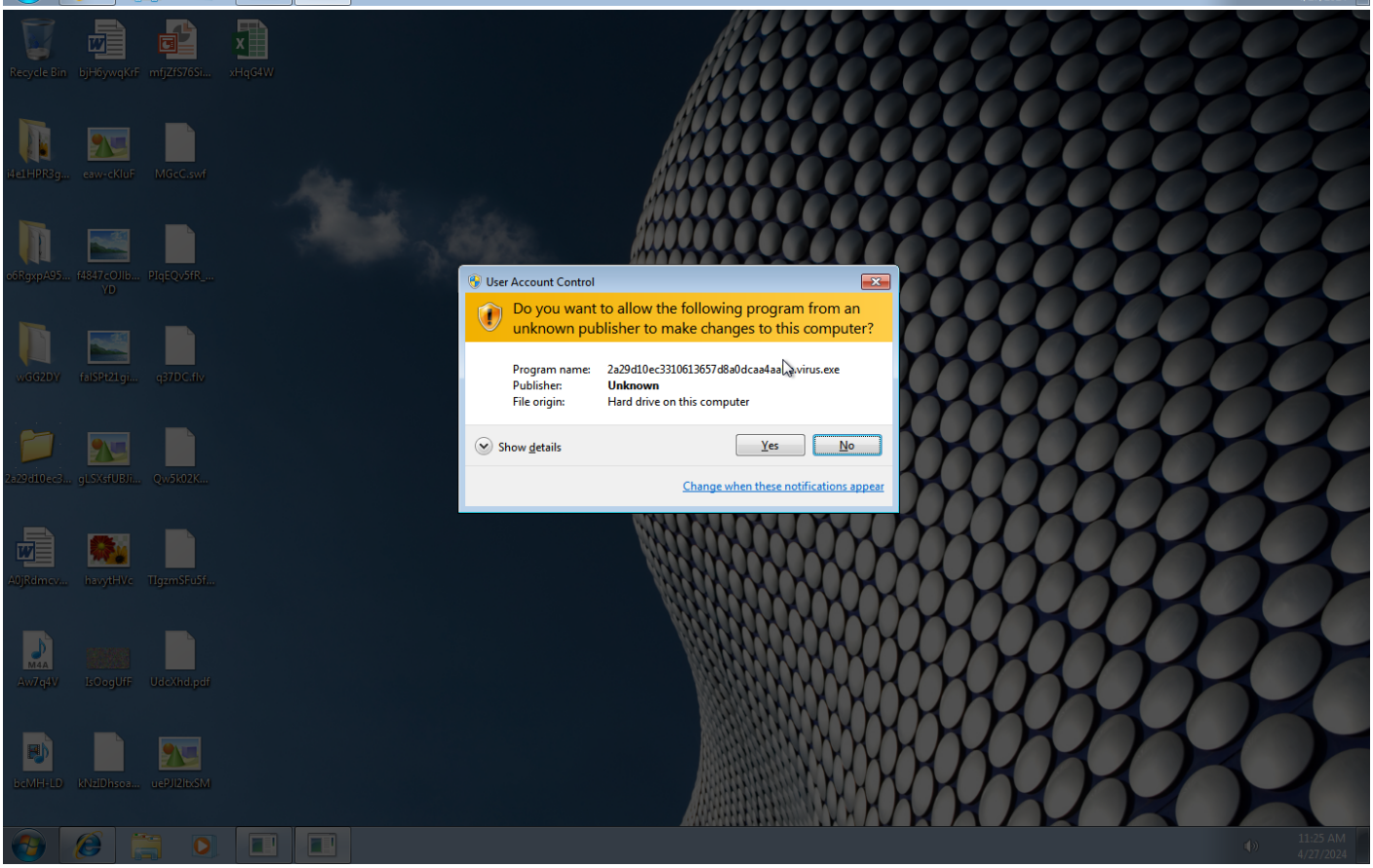
Sample Information

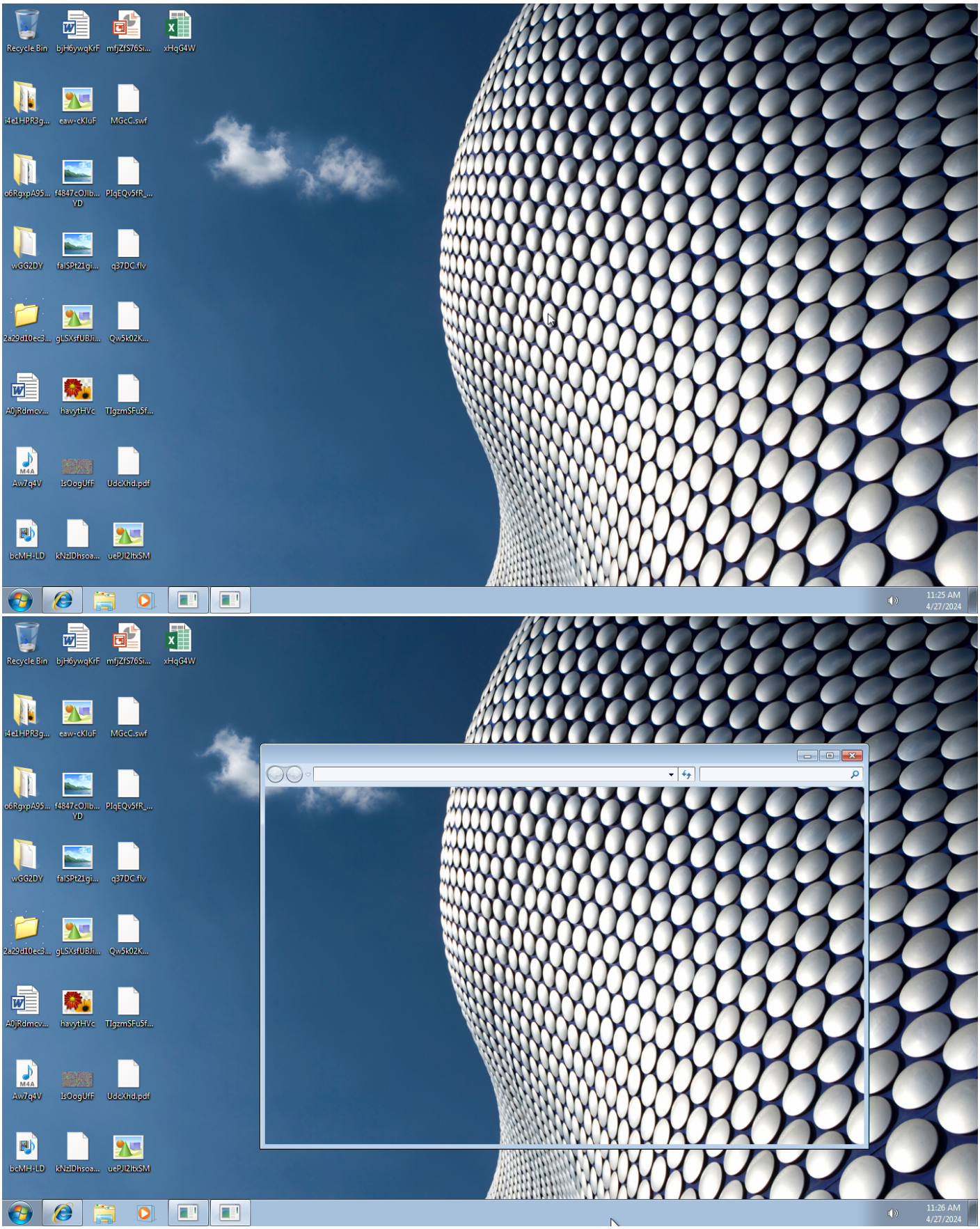
ID	#10314539
MD5	2a29d10ec3310613657d8a0dcaa4aabe
SHA1	f99a7d5d2ce42d5bb5ddc4c66db6ed7eb8d9bb58
SHA256	05b8805d514836fe3de91c1a34ba61a97c9c9ab46f380b65f81ab26cb1cb63d5
SSDeep	393216:w8zIZAhNURa8zIZAhNURm8zIZAhNURa8zIZAhNURR8zIZAhNURa8zIZAhNURm8zp:w8zIZGUa8zIZGUm8zIZGUa8zIZGUR8zV
ImpHash	85de11416899930380628ef20827d5fe
File Name	2a29d10ec3310613657d8a0dcaa4aabe.virus.exe
File Size	20745.32 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-04-27 09:25 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	12
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
bjH6ywqKrF
mfjZfS76Si...
xHqG4W
i4e1HPR3g...
eaw-cKluF
MGcC.swf
o6RgxpA95...
f4847cOJlb...
YD
PlqEQv5fR_...
wGG2DY
faiSPt21gi...
q37DC.flv
2a29d10ec3...
gLSXsfUBJr...
Qw5k02K...
A0jRdmcv...
havytHVc
TIgzmSFu5f...
Aw7q4V
IsOogUfF
UdcXhd.pdf
bcMH-LD
kNzlDhsoa...
uePJl2lbSM
11:25 AM
4/27/2024


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 2a29d10ec3310613657d8a0dcaa4aa...virus.exe
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

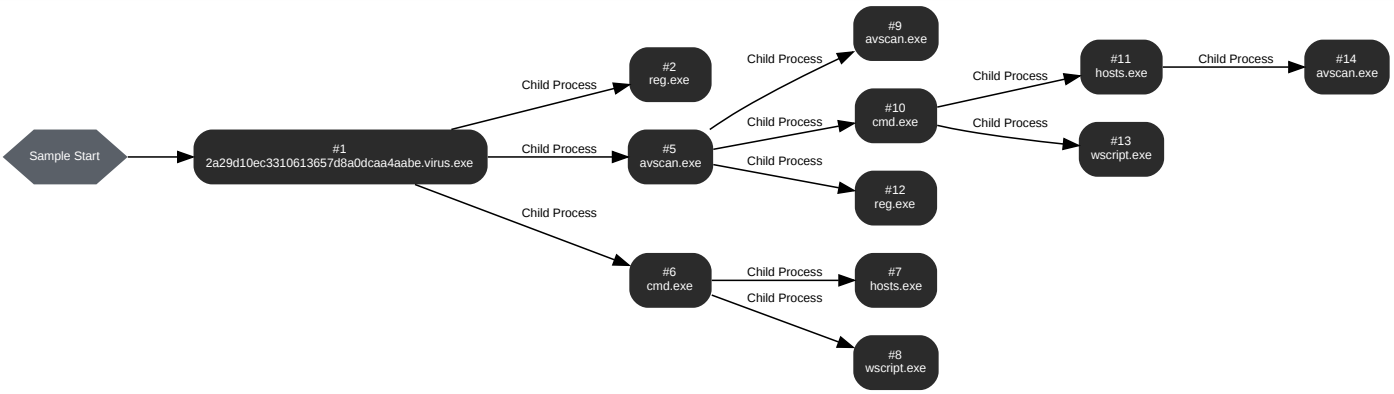
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\2a29d10ec3310613657d8a0dcaa4aabe.virus.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\2a29d10ec3310613657d8a0dcaa4aabe.virus.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51394, Reason: Analysis Target
Unmonitor End Time	End Time: 136329, Reason: Terminated
Monitor duration	84.94s
Return Code	0
PID	3892
Parent PID	-
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\windows\W_X_C.vbs	197 bytes	62894ee80c01474985035813efed6424d22326ea4a92ccfa0718a76875456284	✖
\??\c:\users\keecfmwgj\appdata\local\temp\avscan.exe	10240.00 KB	5ce56e05da8bca57172ec476d9492c4c78f0dcdd9d3ca6881fa2eaa6660e4129	✖
c:\windows\W_X_C.bat	336 bytes	d2150b9e5a4ce55e140f0ca91c4e300715d42095c8fddf58c77037cdd2cfaf78	✖

Host Behavior

Type	Count
System	718
Module	778
Environment	1
File	124
-	7
Mutex	1
Keyboard	5
Registry	21
-	8
User	1
-	1
Window	16
COM	6
Process	3
-	2

Process #2: reg.exe

ID	2
File Name	c:\windows\syswow64\reg.exe
Command Line	REG DELETE HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot /f
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85129, Reason: Child Process
Unmonitor End Time	End Time: 86861, Reason: Terminated
Monitor duration	1.73s
Return Code	1
PID	3940
Parent PID	3892
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	369
File	10

Process #5: avscan.exe

ID	5
File Name	c:\users\keecfmwgj\appdata\local\temp\avscan.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106568, Reason: Child Process
Unmonitor End Time	End Time: 301902, Reason: Terminated by timeout
Monitor duration	195.33s
Return Code	Unknown
PID	4052
Parent PID	3892
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\A0jRdmcvV1haBm5.doc	10240.00 KB	5ce56e05da8bca57172ec476d9492c4c78f0dcdd9d3ca6881fa2eaa6660e4129	✖

Host Behavior

Type	Count
System	2729
Module	821
Environment	1
File	131
-	7
Mutex	1
Keyboard	5
Registry	16
-	58
User	1
-	1
Window	15
COM	12
Process	3

Process #6: cmd.exe

ID	6
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c c:\windows\W_X_C.bat
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133048, Reason: Child Process
Unmonitor End Time	End Time: 141684, Reason: Terminated
Monitor duration	8.64s
Return Code	0
PID	4064
Parent PID	3892
Bitness	32 Bit

Host Behavior

Type	Count
Module	7
Environment	2
File	66
Process	3
-	1

Process #7: hosts.exe

ID	7
File Name	c:\windows\hosts.exe
Command Line	C:\windows\hosts.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135487, Reason: Child Process
Unmonitor End Time	End Time: 301902, Reason: Crashed
Monitor duration	166.41s
Return Code	Unknown
PID	2720
Parent PID	4064
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
Environment	1
File	6
-	1
Mutex	1

Process #8: wscript.exe

ID	8
File Name	c:\windows\syswow64\wscript.exe
Command Line	"C:\Windows\System32\WScript.exe" "C:\Windows\W_X_C.vbs"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140357, Reason: Child Process
Unmonitor End Time	End Time: 146765, Reason: Terminated
Monitor duration	6.41s
Return Code	0
PID	2924
Parent PID	4064
Bitness	32 Bit

Host Behavior

Type	Count
System	14
Module	20
Registry	29
-	1
Window	2
COM	5
File	3

Process #9: avscan.exe

ID	9
File Name	c:\users\keecfmwgj\appdata\local\temp\avscan.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148214, Reason: Child Process
Unmonitor End Time	End Time: 166990, Reason: Terminated
Monitor duration	18.78s
Return Code	0
PID	2988
Parent PID	4052
Bitness	32 Bit

Host Behavior

Type	Count
System	79
Module	445
Environment	1
File	108
-	7
Mutex	1
Registry	15
Keyboard	4
-	2
User	1
-	1
Window	15
COM	2
-	2

Process #10: cmd.exe

ID	10
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c c:\windows\W_X_C.bat
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 165561, Reason: Child Process
Unmonitor End Time	End Time: 173519, Reason: Terminated
Monitor duration	7.96s
Return Code	0
PID	2940
Parent PID	4052
Bitness	32 Bit

Host Behavior

Type	Count
Module	7
Environment	1
File	49
Process	1

Process #11: hosts.exe

ID	11
File Name	c:\windows\hosts.exe
Command Line	C:\windows\hosts.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 166992, Reason: Child Process
Unmonitor End Time	End Time: 301902, Reason: Terminated by timeout
Monitor duration	134.91s
Return Code	Unknown
PID	2888
Parent PID	2940
Bitness	32 Bit

Host Behavior

Type	Count
System	1125
Module	492
Environment	1
File	105
-	7
Mutex	1
Registry	10
Keyboard	4
-	27
User	1
-	1
Window	15
COM	2
Process	1

Process #12: reg.exe

ID	12
File Name	c:\windows\syswow64\reg.exe
Command Line	REG DELETE HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot /f
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 172029, Reason: Child Process
Unmonitor End Time	End Time: 177762, Reason: Terminated
Monitor duration	5.73s
Return Code	1
PID	3280
Parent PID	4052
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	337
File	10

Process #13: wscript.exe

ID	13
File Name	c:\windows\syswow64\wscript.exe
Command Line	"C:\Windows\System32\WScript.exe" "C:\Windows\W_X_C.vbs"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 172217, Reason: Child Process
Unmonitor End Time	End Time: 178208, Reason: Terminated
Monitor duration	5.99s
Return Code	0
PID	3332
Parent PID	2940
Bitness	32 Bit

Host Behavior

Type	Count
System	14
Module	20
Registry	29
-	1
Window	2
COM	5
File	3

Process #14: avscan.exe

ID	14
File Name	c:\users\keecfmwgj\appdata\local\temp\avscan.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 197633, Reason: Child Process
Unmonitor End Time	End Time: 301902, Reason: Terminated by timeout
Monitor duration	104.27s
Return Code	Unknown
PID	3412
Parent PID	2888
Bitness	32 Bit

Host Behavior

Type	Count
System	17
Module	274
Environment	1
File	6
-	6
Mutex	1
Keyboard	4
Registry	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
05b8805d514836fe3de91c1a34ba61a97c9c9ab46f380b65f81ab26cb1cb63d5	C:\Users\kEecfMwgj\Desktop\2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, \??\c:\users\keecfmwgj\desktop\2a29d10ec3310613657d8a0dcaa4aabe.virus.exe	Sample File	20745.32 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
d2150b9e5a4ce55e140f0ca91c4e300715d42095c8fddf58c77037cdd2cfaf78	c:\windows\W_X_C.bat	Dropped File	336 bytes	text/x-msdos-batch	Access, Create, Read, Write	MALICIOUS
5ce56e05da8bca57172ec476d9492c4c78f0dcdd9d3ca6881fa2eaa6660e4129	C:\Users\kEecfMwgj\Desktop\A0jRdmcvV1haBm5.doc, \??\c:\users\keecfmwgj\appdata\local\temp\avscan.exe, C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe, C:\Windows\hosts.exe, C:\windows\hosts.exe, \??\c:\windows\hosts.exe	Dropped File	10240.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
62894ee80c01474985035813efed6424d22326ea4a92ccfa0718a76875456284	C:\windows\W_X_C.vbs, C:\Windows\W_X_C.vbs	Dropped File	197 bytes	text/plain	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\2a29d10ec3310613657d8a0dcaa4aabe.virus.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\windows\W_X_C.vbs	Accessed File, Dropped File	Access, Create, Write	CLEAN
c:\windows\W_X_C.bat	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
\??\c:\users\keecfmwgj\appdata\local\temp\avscan.exe	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Windows\hosts.exe	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Windows\system32\MSVBVM60.DLL	Accessed File	Access	CLEAN
.	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp	Accessed File	Access	CLEAN
\\.\C:	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\temp\80EB2F5C	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
WINHELP.INI	Accessed File	Access, Read	CLEAN
C:\Windows\system32\.HLP	Accessed File	Access	CLEAN
C:\Windows\Help\.HLP	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WScript.exe	Accessed File	Access	CLEAN
W_X_C.bat	Miscellaneous File	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Borland\Locales	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\EnigmaDevelopers	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_CURRENT_USER\Software\Enigma Protector\29AEB4A0365755F6-B862CAE984EA4D0E\02F01F553A112DCE-00C9DB38C18D5FD1	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors	access	hosts.exe, 2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\avscan	write, access	2a29d10ec3310613657d8a0dcaa4aabe.virus.exe, avscan.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\AppInfo	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\AppMgmt	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Base	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Boot Bus Extender	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Boot file system	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\CryptSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\DcomLaunch	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\EFS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\EventLog	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\File system	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Filter	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\HelpSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\KeyIso	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Netlogon	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\NTDS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\PCI Configuration	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\PlugPlay	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\PNP Filter	access	reg.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Power	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Primary disk	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\ProfSvc	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\RpcEptMapper	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\RpcSs	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\sacsvr	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SCSI Class	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\sermouse.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SWPRV	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\System Bus Extender	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TabletInputService	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TBS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TrustedInstaller	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\VDS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\vga.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\vgasave.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\vmms	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\volmgr.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\volmgrx.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\WinDefend	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\WinMgmt	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\WudfPf	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\WudfRd	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\WudfSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{36FC9E60-C465-11CF-8056-444553540000}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E965-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E969-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E96A-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E96B-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E96F-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E977-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E97B-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E97D-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E980-E325-11CE-BFC1-08002BE10318}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{533C5B84-EC70-11D2-9505-00C04F79DEAF}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{6BDD1FC1-810F-11D0-BEC7-08002BE2092F}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{71A27CDD-812A-11D0-BEC7-08002BE2092F}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{745A17A0-74D3-11D0-B6FE-00A0C90F57DA}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{D48179BE-EC20-11D1-B6B8-00C04FA372A7}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{D94EE5D8-D189-4994-83D2-F68D7D41B0E6}	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AFD	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AppInfo	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AppMgmt	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Base	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\BFE	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Boot Bus Extender	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Boot file system	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\bowser	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Browser	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CryptSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\DcomLaunch	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\dfsc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Dhcp	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\DnsCache	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Dot3Svc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Eaphost	access	reg.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EFS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EventLog	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\File system	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Filter	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\HelpSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\IKEEXT	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\ipnat.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\KeyIso	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\LanmanServer	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\LanmanWorkstation	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\LmHosts	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Messenger	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\MPSDrv	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\MPSSvc	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\mrxsmb	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\mrxsmb10	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\mrxsmb20	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NativeWifiP	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NDIS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NDIS Wrapper	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\ndiscap	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Ndisuio	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NetBIOS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NetBIOSGroup	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NetBT	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NetDDEGroup	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Netlogon	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NetMan	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\netprofm	access	reg.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Network	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NetworkProvider	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NlaSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Nsi	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\nsiproxy.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\NTDS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\PCI Configuration	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\PlugPlay	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\PNP Filter	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\PNP_TDI	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\PolicyAgent	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Power	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Primary disk	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\ProfSvc	delete, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\rdbss	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\rdpencdd.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\rdsessmgr	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\RpcEptMapper	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\RpcSs	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\sacsvr	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SCardSvr	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SCSI Class	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\sermouse.sys	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SharedAccess	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Streams Drivers	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SWPRV	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\System Bus Extender	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TabletInputService	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TBS	access	reg.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Tcpip	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TDI	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TrustedInstaller	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\VaultSvc	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\VDS	access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\vga.sys	access	reg.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
2a29d10ec3310613657d8a0dcaa4aabe.virus.exe	"C:\Users\kEecfMwgj\Desktop\2a29d10ec3310613657d8a0dcaa4aabe.virus.exe"	MALICIOUS
avscan.exe	C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe	MALICIOUS
cmd.exe	C:\Windows\system32\cmd.exe /c c:\windows\W_X_C.bat	SUSPICIOUS
avscan.exe	C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe	SUSPICIOUS
cmd.exe	C:\Windows\system32\cmd.exe /c c:\windows\W_X_C.bat	SUSPICIOUS
hosts.exe	C:\windows\hosts.exe	SUSPICIOUS
wscript.exe	"C:\Windows\System32\WScript.exe" "C:\Windows\W_X_C.vbs"	CLEAN
avscan.exe	C:\Users\KEECFM~1\AppData\Local\Temp\avscan.exe	CLEAN
reg.exe	REG DELETE HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot /f	CLEAN
hosts.exe	C:\windows\hosts.exe	CLEAN
wscript.exe	"C:\Windows\System32\WScript.exe" "C:\Windows\W_X_C.vbs"	CLEAN
reg.exe	REG DELETE HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot /f	CLEAN

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	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

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