MALICIOUS

Classifications: Backdoor

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**SecuriteInfo.com.Trojan-PSW.Agent.26016.exe**
ID	#9868679
MD5	c9a36a7e0bf431dafe139b1cc18609ed
SHA1	4d77f0d31e994d3baeba164238634cadaf95fb77
SHA256	7e33dd313ed09a15c81af55ee0997031caa3da8fba8c31c3859bc95e52559ff3
File Size	4269.50 KB
Report Created	2024-02-11 21:14 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 34 matches)

Score	Category	Operation	Count	Classification
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample enumerates processes, collects hardware information and queries network configuration which indicates system fingerprinting.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #2) wmic.exe queries hardware properties via WMI: SELECT Name FROM WIN32_PROCESSOR. • (Process #6) wmic.exe queries hardware properties via WMI: SELECT Name FROM win32_VideoController.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Searches for sensitive browser data	13	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Amigo" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Torch" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Uran" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Chrome Canary" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "7Star" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe searches for sensitive data of web browser "Kometa" by file.			
2/5	Network Connection	Sets up server that accepts incoming connections	2	Backdoor
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe starts a TCP server listening on port 49163. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe starts a TCP server listening on port 49162.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe enumerates running processes.			
1/5	Discovery	Reads system data	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe reads the cryptographic machine GUID from registry.			

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe starts (process #2) wmic.exe with a hidden window. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe starts (process #6) wmic.exe with a hidden window.			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe tries to gather information about application "FileZilla" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe resolves hostname "ipinfo.io" to IP "34.117.186.192". • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe resolves hostname "hzp02itt0a.com" to IP "193.178.170.30".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe opens an outgoing TCP connection to host "193.178.170.30:80". • (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe opens an outgoing TCP connection to host "34.117.186.192:80".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe resolves 253 API functions by name.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #1) securiteinfo.com.trojan-psw.agent.26016.exe checks external IP by asking IP info service at "http://ipinfo.io".			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

Mitre ATT&CK Matrix

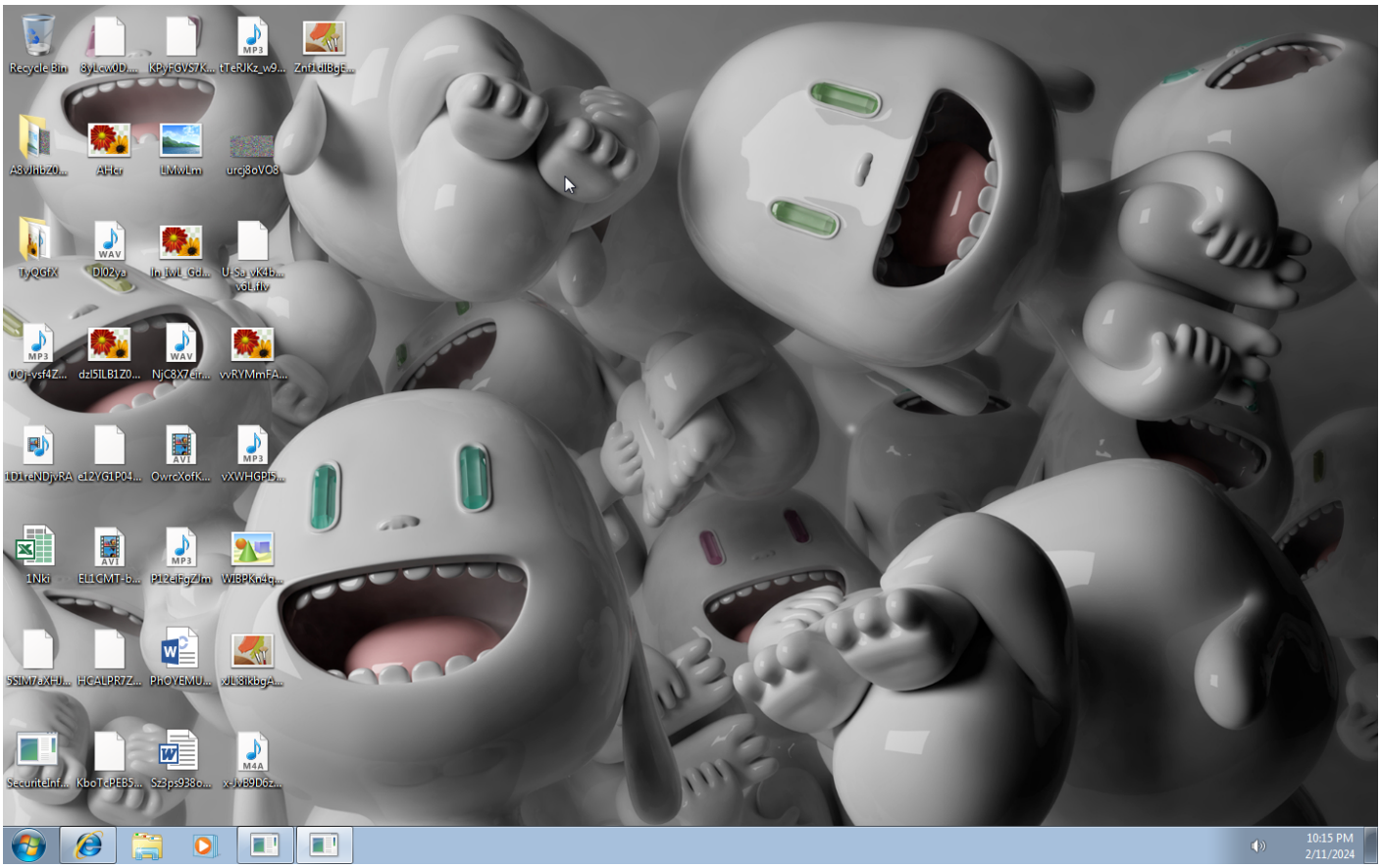
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection			
				#T1143 Hidden Window		#T1057 Process Discovery		#T1005 Data from Local System			
				#T1045 Software Packing		#T1082 System Information Discovery					
						#T1012 Query Registry					
						#T1083 File and Directory Discovery					
						#T1016 System Network Configuration Discovery					

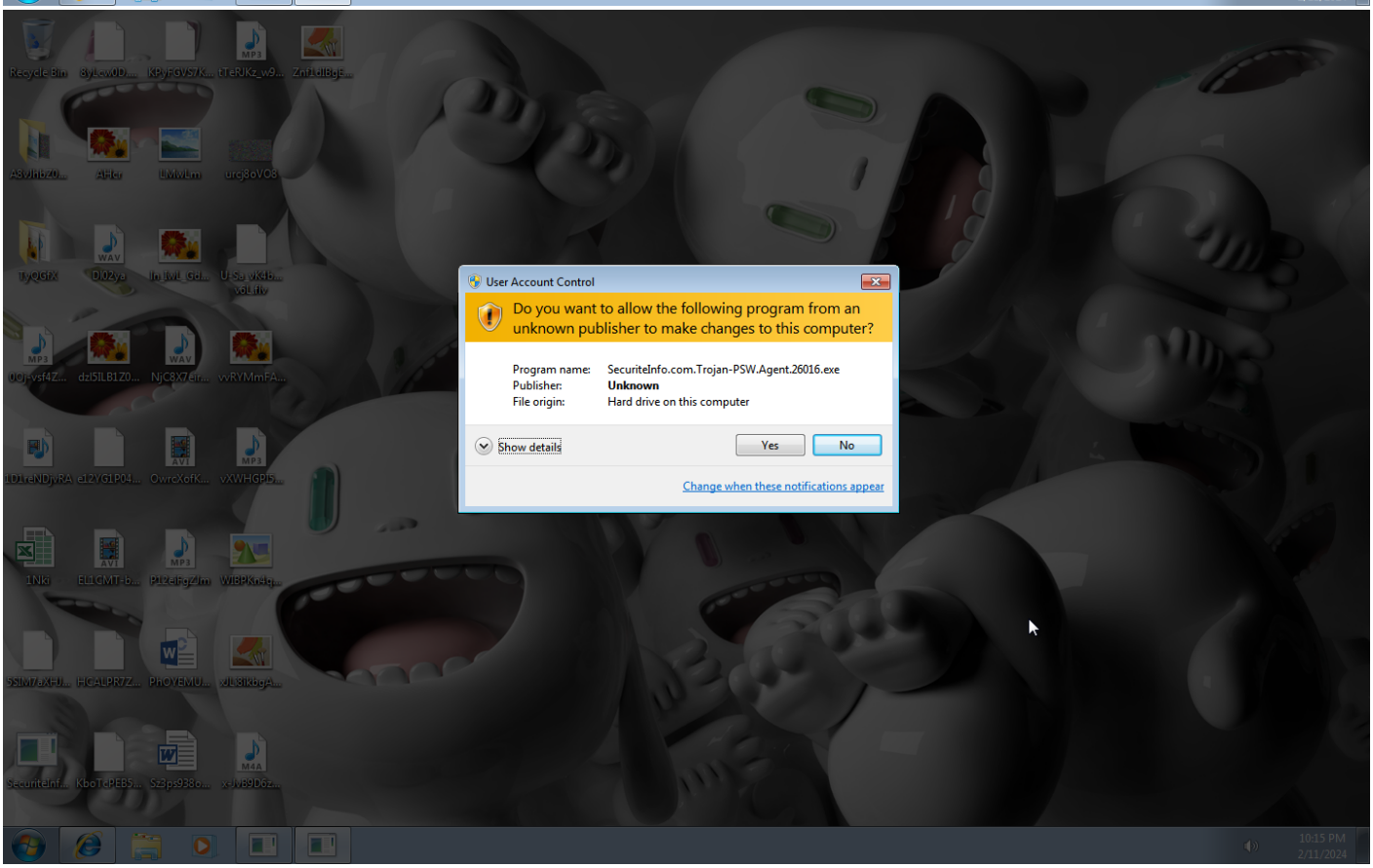
Sample Information

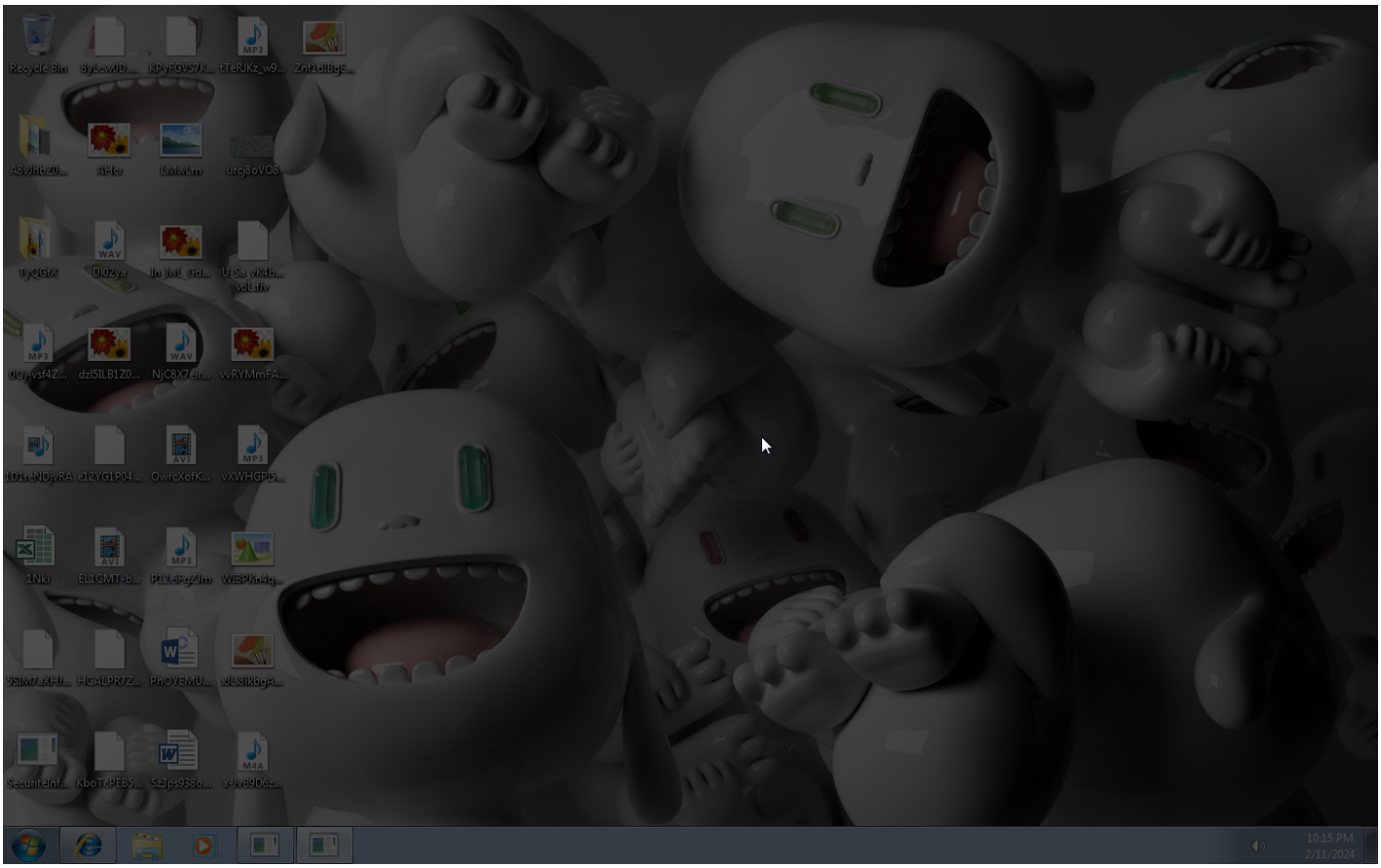
ID	#9868679
MD5	c9a36a7e0bf431dafe139b1cc18609ed
SHA1	4d77f0d31e994d3baeba164238634cadaf95fb77
SHA256	7e33dd313ed09a15c81af55ee0997031caa3da8fba8c31c3859bc95e52559ff3
SSDeep	98304:6PSzwcdHYUcyX4eHU0hU/cSuijBf1ULKPQ1w9VOO6GQgjIkU:WS0cJ59U0hUkx6f1g1w9CGQ2I
ImpHash	9aebf3da4677af9275c461261e5abde3
File Name	SecuriteInfo.com.Trojan-PSW.Agent.26016.exe
File Size	4269.50 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

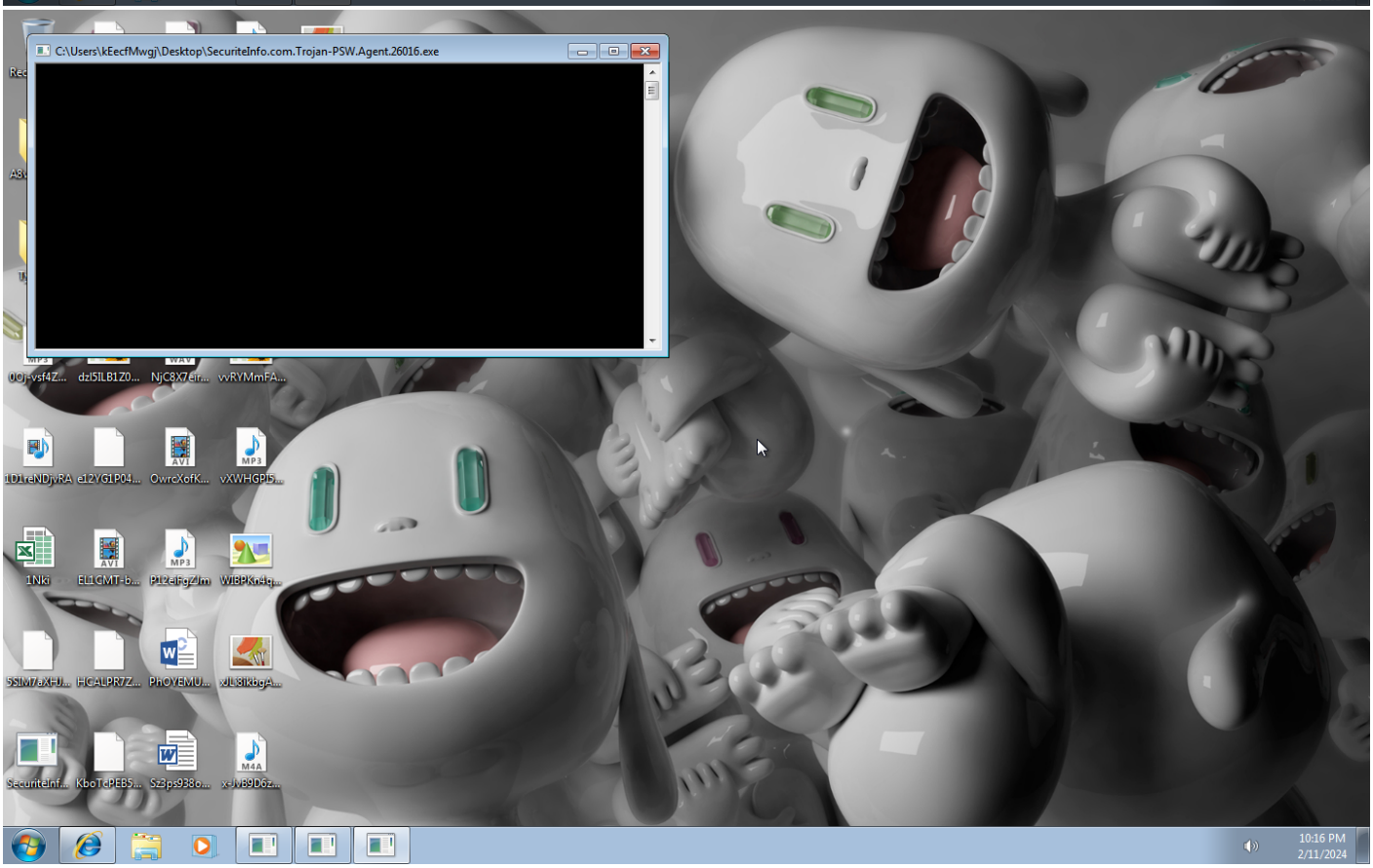
Analysis Information

Creation Time	2024-02-11 21:14 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	5
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




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: SecuriteInfo.com.Trojan-PSW.Agent.26016.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1.95 KB total sent

2.27 KB total received

3 ports 80, 53, 445

3 contacted IP addresses

0 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

2 sessions, 1.83 KB sent, 2.04 KB received

HTTP Requests

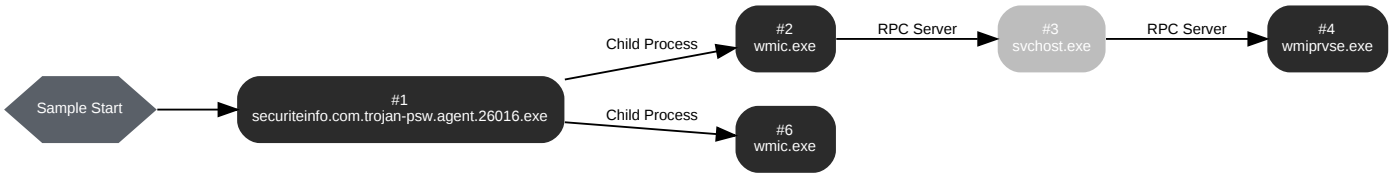
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://ipinfo[.]io	-	-	-	0 bytes	CLEAN
POST	hxxp://hzp02itt0a[.]com/submit/info	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	ipinfo[.]io	NO_ERROR	34.117.186.192	-	CLEAN
A	hzp02itt0a[.]com	NO_ERROR	193.178.170.30	-	CLEAN

BEHAVIOR

Process Graph



Process #1: securiteinfo.com.trojan-psw.agent.26016.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\securiteinfo.com.trojan-psw.agent.26016.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\SecuriteInfo.com.Trojan-PSW.Agent.26016.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67121, Reason: Analysis Target
Unmonitor End Time	End Time: 139515, Reason: Terminated
Monitor duration	72.39s
Return Code	0
PID	3444
Parent PID	1912
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\system.txt	547 bytes	28af184aa962040cdbd0d8a4e4e48c11e9217fe1485672e06587d8a4ae62ddcb	✖
C:\Users\KEECFM~1\AppData\Local\Temp\cM5o6GeI.zip	451 bytes	c6b1ac621b3769171b98370ac29ba6a6edc4f0027ebf438fd83eddbde68b8460	✖

Host Behavior

Type	Count
Module	307
System	17
Environment	76
-	15
File	388
User	2
Process	769
Registry	8
-	8
-	2

Network Behavior

Type	Count
HTTP	2
DNS	2
TCP	2

Process #2: wmic.exe

ID	2
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic cpu get name
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 115456, Reason: Child Process
Unmonitor End Time	End Time: 120823, Reason: Terminated
Monitor duration	5.37s
Return Code	0
PID	3564
Parent PID	3444
Bitness	64 Bit

Host Behavior

Type	Count
System	14
Module	5
COM	8
Registry	5
File	8
-	1

Process #3: svchost.exe

ID	3
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 117694, Reason: RPC Server
Unmonitor End Time	End Time: 308116, Reason: Terminated by timeout
Monitor duration	190.42s
Return Code	Unknown
PID	876
Parent PID	3564
Bitness	64 Bit

Process #4: wmiprvse.exe

ID	4
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 117694, Reason: RPC Server
Unmonitor End Time	End Time: 308116, Reason: Terminated by timeout
Monitor duration	190.42s
Return Code	Unknown
PID	2680
Parent PID	876
Bitness	64 Bit

Host Behavior

Type	Count
System	1

Process #6: wmic.exe

ID	6
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic path win32_VideoController get name
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 119934, Reason: Child Process
Unmonitor End Time	End Time: 123411, Reason: Terminated
Monitor duration	3.48s
Return Code	0
PID	3596
Parent PID	3444
Bitness	64 Bit

Host Behavior

Type	Count
System	14
Module	5
COM	8
Registry	5
File	8
-	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7e33dd313ed09a15c81af55ee0997031caa3da8fba8c31c3859bc95e52559ff3	C:\Users\kEecfMwgj\Desktop\SecuriteInfo.com.Trojan-PSW.Agent.26016.exe	Sample File	4269.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0d3c8dd6f6eadcaf754042a5d0dbdaadc6fac385b91f9c3926a7dc393614c392	-	Downloaded File	310 bytes	application/json	-	CLEAN
85599a07279c398837833e65ce849274ad5c31ee700858a41602dcdd414644a4	-	Downloaded File	1.11 KB	application/json	-	CLEAN
74234e98afe7498fb5daf1f36ac2d78acc339464f950703b8c019892f982b90b	-	Downloaded File	4 bytes	text/plain	-	CLEAN
28af184aa962040cdbd0d8a4e4e48c11e9217fe1485672e06587d8a4ae62ddcb	C:\Users\KEECFM~1\AppData\Local\Temp\system.txt, system.txt	Archive File	547 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
c6b1ac621b3769171b98370ac29ba6a6edc4f0027ebf438fd83eddbde68b8460	C:\Users\KEECFM~1\AppData\Local\Temp\cM5o6GeI.zip	Dropped File	451 bytes	application/zip	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\SecuriteInfo.com.Trojan-PSW.Agent.26016.exe	Sample File	-	MALICIOUS
C:\Users\KEECFM~1\AppData\Local\Temp\system.txt	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
system.txt	Miscellaneous File	-	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\cM5o6GeI.zip	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
wmic.com	Accessed File	Access	CLEAN
wmic.exe	Accessed File	Access	CLEAN
wmic.bat	Accessed File	Access	CLEAN
wmic.cmd	Accessed File	Access	CLEAN
wmic.vbs	Accessed File	Access	CLEAN
wmic.vbe	Accessed File	Access	CLEAN
wmic.js	Accessed File	Access	CLEAN
wmic.jse	Accessed File	Access	CLEAN
wmic.wsf	Accessed File	Access	CLEAN
wmic.wsh	Accessed File	Access	CLEAN
wmic.msc	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.com	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.bat	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.cmd	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.vbs	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.vbe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.js	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.jse	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.wsf	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.wsh	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Oracle\Java\javapath\wmic.msc	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.com	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.exe	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.bat	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.cmd	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.vbs	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.vbe	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.js	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.jse	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.wsf	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.wsh	Accessed File	Access	CLEAN
C:\Windows\system32\wmic.msc	Accessed File	Access	CLEAN
C:\Windows\wmic.com	Accessed File	Access	CLEAN
C:\Windows\wmic.exe	Accessed File	Access	CLEAN
C:\Windows\wmic.bat	Accessed File	Access	CLEAN
C:\Windows\wmic.cmd	Accessed File	Access	CLEAN
C:\Windows\wmic.vbs	Accessed File	Access	CLEAN
C:\Windows\wmic.vbe	Accessed File	Access	CLEAN
C:\Windows\wmic.js	Accessed File	Access	CLEAN
C:\Windows\wmic.jse	Accessed File	Access	CLEAN
C:\Windows\wmic.wsf	Accessed File	Access	CLEAN
C:\Windows\wmic.wsh	Accessed File	Access	CLEAN
C:\Windows\wmic.msc	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\wmic.com	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem\wmic.exe	Accessed File	Access	CLEAN
NUL	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\XSL-Mappings.xml	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\\texttable.xsl	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\Cookies	Accessed File	Access, Create, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Edge\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\BraveSoftware\Brave-Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Amigo\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Torch\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex\YandexBrowser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\uCozMedia\Uran\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Epic Privacy Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome SxS\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome SxS\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Vivaldi\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Sputnik\Sputnik\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\7Star\7Star\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CentBrowser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Orbitum\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Kometa\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Mozilla\Firefox\Profiles	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming/discord/Local Storage/leveldb/	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming/discord/Local State	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming/discordptb/Local Storage/leveldb/	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming/discordptb/Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming/discordcanary/Local Storage/leveldb/	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming/discordcanary/Local State	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Exodus	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Coinomi	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Documents\Monero	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\atomic	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Electrum	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\exodus	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\autofills.txt	Accessed File	Access, Delete	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\passwords.txt	Accessed File	Access, Delete	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\bookmarks.txt	Accessed File	Access, Delete	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\cards.txt	Accessed File	Access, Delete	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\discord-tokens.txt	Accessed File	Access, Delete	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\exodus-passwords.txt	Accessed File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\intentlauncher\launcherconfig	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\.lunarclient\settings\game\accounts.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.minecraft\TlauncherProfiles.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.feather\accounts.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.minecraft\meteor-client\accounts.nbt	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.minecraft\Impact\alts.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.minecraft\Novoline\alts.novo	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.minecraft\launcher_accounts_microsoft_store.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\.minecraft\Rise\alts.txt	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\intentlauncher\Rise\alts.txt	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\paladium-group\accounts.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\PolyMC\accounts.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Badlion Client\accounts.json	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Exodus\exodus.wallet	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\coinomi\coinomi\wallets	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Tox	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Documents\Monero\wallets	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\atomic\databases	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Roaming\Electrum\wallets	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Telegram Desktop\tdata	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Signal	Accessed File	Access	CLEAN
C:\Program Files (x86)\Steam\config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://ipinfo[.]io	Extracted, Contacted	34.117.186.192	United States	GET	CLEAN
hxxp://hzp02itt0a[.]com/submit/info	Extracted, Contacted	193.178.170.30	Russia	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
ipinfo[.]io	34.117.186.192	United States	HTTP, TCP, DNS	CLEAN
hzp02itt0a[.]com	193.178.170.30	Russia	HTTP, TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
34.117.186.192	ipinfo[.]io	United States	HTTP, TCP, DNS	CLEAN
193.178.170.30	hzp02itt0a[.]com	Russia	HTTP, TCP, DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	securiteinfo.com.trojan-psw.agent.26016.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	access, read	securiteinfo.com.trojan-psw.agent.26016.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	access, read	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	securiteinfo.com.trojan-psw.agent.26016.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	access, read	securiteinfo.com.trojan-psw.agent.26016.exe	CLEAN
HKEY_CURRENT_USER\Software\iPwonTCGCC	access, create	securiteinfo.com.trojan-psw.agent.26016.exe	CLEAN
HKEY_CURRENT_USER\Software\iPwonTCGCC\ID	write, access	securiteinfo.com.trojan-psw.agent.26016.exe	CLEAN

Process

Process Name	Commandline	Verdict
securiteinfo.com.trojan-psw.agent.26016.exe	"C:\Users\kEecfMwgj\Desktop\SecuriteInfo.com.Trojan-PSW.Agent.26016.exe"	MALICIOUS
wmic.exe	wmic cpu get name	SUSPICIOUS
wmic.exe	wmic path win32_VideoController get name	SUSPICIOUS

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	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	2024.1.0
Dynamic Engine Version	2024.1.0 / 01/04/2024 17:31
Static Engine Version	2024.1.0.0 / 2024-01-04 16:05:55
AV Exceptions Version	2024.1.2.19 / 2024-01-30 23:09:03
Link Detonation Heuristics Version	2024.1.2.20 / 2024-02-01 16:04:36
Smart Memory Dumping Rules Version	2024.1.2.19 / 2024-01-30 23:09:03
Config Extractors Version	2024.1.2.20 / 2024-02-01 16:04:36
Signature Trust Store Version	2024.1.2.19 / 2024-01-30 23:09:03
VMRay Threat Identifiers Version	2024.1.2.20 / 2024-02-01 16:04:36
YARA Built-in Ruleset Version	2024.1.2.21

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