MALICIOUS

Classifications: Spyware, Injector

Threat Names: Mal/Generic-S, AgentTesla, AgentTesla.v4

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Draft Itinerary 2024 tour plan - A Best Outbound client.exe**
ID	#9819794
MD5	65bcf2c6ef1e115e4cc4e15e5a83bdfb
SHA1	e5830a23d3f18a44d99d34f1e8126283ab9a8caa
SHA256	ac71f9ab4ccb920a493508b0e0577b31fe547aa07e914f58f1def47d08ebcf7d
File Size	1077.57 KB
Report Created	2024-02-06 12:16 (UTC+1)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (25 rules, 37 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
	• A configuration for Agent Tesla was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• YARA detected "AgentTesla_HTML_Message" from ruleset "Malware" in memory dump data from (process #2) aspnet_compiler.exe.			
5/5	Discovery	Combination of other detections shows configuration discovery	1	-
	• Sample queries network configuration, collects hardware information and collects operating system information which indicates system fingerprinting.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) draft itinerary 2024 tour plan - a best outbound client.exe modifies memory of (process #2) aspnet_compiler.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) draft itinerary 2024 tour plan - a best outbound client.exe alters context of (process #2) aspnet_compiler.exe.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Execution	Sends control codes to a driver	3	-
	• (Process #4) wmiprvse.exe controls driver "\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}" through API DeviceIOControl. • (Process #4) wmiprvse.exe controls driver "\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}" through API DeviceIOControl. • (Process #4) wmiprvse.exe controls driver "\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}" through API DeviceIOControl.			
2/5	Anti Analysis	Tries to detect application sandbox	3	-
	• (Process #2) aspnet_compiler.exe tries to detect "Sandboxie" by checking for existence of module "SbieDll.dll". • (Process #2) aspnet_compiler.exe tries to detect "AVAST Sandbox" by checking for existence of module "snxhk.dll". • (Process #2) aspnet_compiler.exe tries to detect "Comodo Sandbox" by checking for existence of module "cmdvrt32.dll".			
2/5	Discovery	Collects hardware properties	3	-
	• (Process #2) aspnet_compiler.exe queries hardware properties via WMI: Select * from Win32_ComputerSystem. • (Process #2) aspnet_compiler.exe queries hardware properties via WMI: SELECT * FROM Win32_VideoController. • (Process #2) aspnet_compiler.exe queries hardware properties via WMI: SELECT * FROM Win32_Processor.			
2/5	Discovery	Searches for sensitive browser data	2	-
	• (Process #2) aspnet_compiler.exe searches for sensitive data of web browser "Opera" by file. • (Process #2) aspnet_compiler.exe searches for sensitive data of web browser "Mozilla Firefox" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #2) aspnet_compiler.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			
2/5	Discovery	Searches for sensitive mail data	1	-
	• (Process #2) aspnet_compiler.exe tries to access sensitive data of mail application "Microsoft Outlook" by registry.			

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) aspnet_compiler.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) aspnet_compiler.exe queries OS version via WMI query: select * from Win32_OperatingSystem.			
2/5	Heuristics	Signed executable failed signature validation	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\Draft Itinerary 2024 tour plan - A Best Outbound client.exe is signed, but signature validation failed.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) draft itinerary 2024 tour plan - a best outbound client.exe starts (process #2) aspnet_compiler.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) draft itinerary 2024 tour plan - a best outbound client.exe reads from (process #2) aspnet_compiler.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) draft itinerary 2024 tour plan - a best outbound client.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #2) aspnet_compiler.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	4	-
	• (Process #2) aspnet_compiler.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #2) aspnet_compiler.exe tries to gather information about application "SeaMonkey" by file. • (Process #2) aspnet_compiler.exe tries to gather information about application "Foxmail" by registry. • (Process #2) aspnet_compiler.exe tries to gather information about application "Opera Mail" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #2) aspnet_compiler.exe resolves hostname "discord.com" to IP "162.159.128.233". • (Process #2) aspnet_compiler.exe resolves hostname "ip-api.com" to IP "208.95.112.1".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #2) aspnet_compiler.exe opens an outgoing TCP connection to host "208.95.112.1:80". • (Process #2) aspnet_compiler.exe opens an outgoing TCP connection to host "162.159.128.233:443".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) aspnet_compiler.exe resolves 50 API functions by name.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #2) aspnet_compiler.exe checks external IP by asking IP info service at "http://ip-api.com/line/?fields=hosting".			
1/5	Crash	A monitored process crashed	1	-
	• (Process #2) aspnet_compiler.exe crashed.			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
URL	Url	https://discord.com/api/webhooks/1202330946817237022/1d5Ynow6yHbMqcRfr75qQjJVcSQnFlKpV4g5H2hHiKoRW33XeyZHnl…

Mitre ATT&CK Matrix

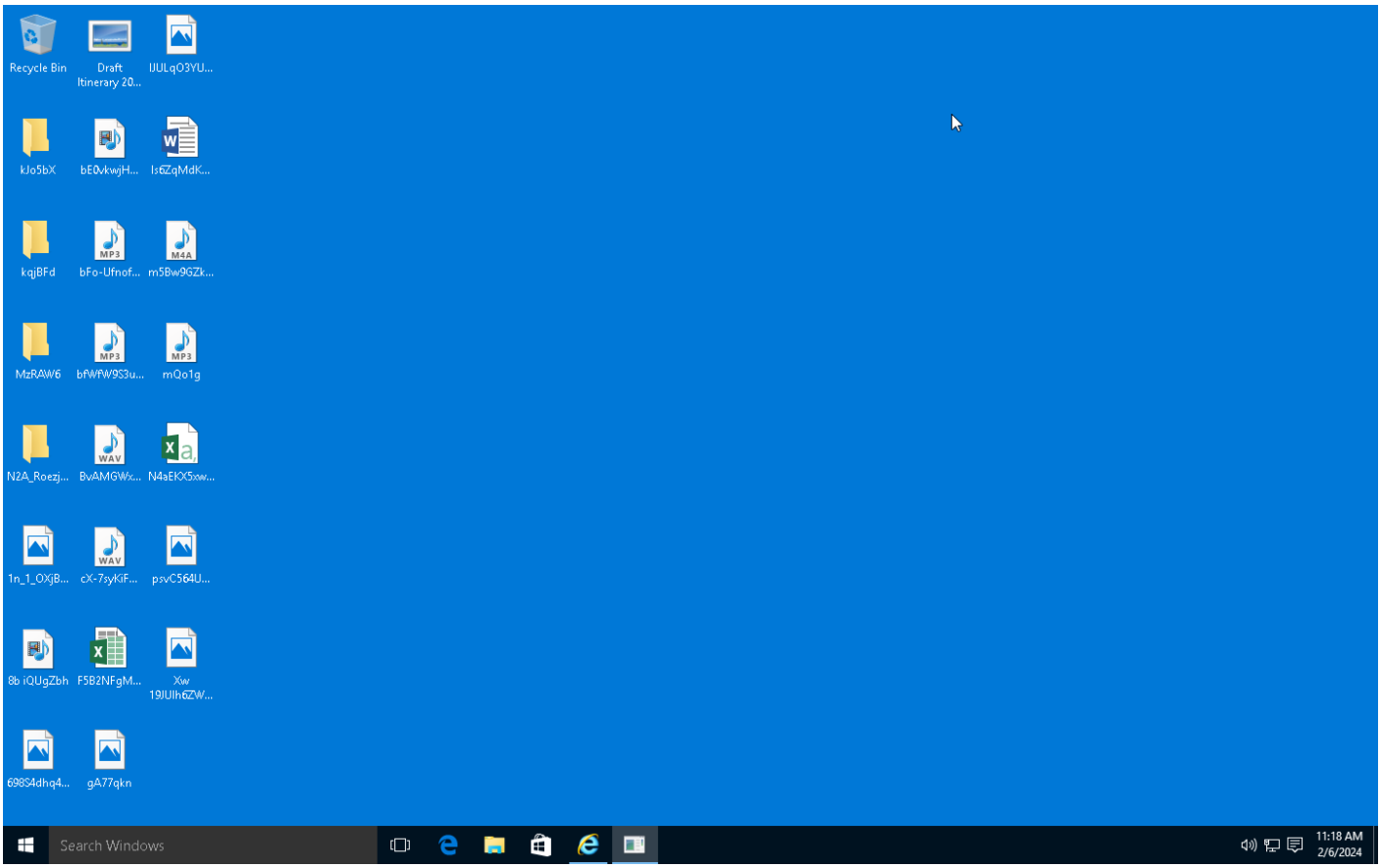
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection			
				#T1045 Software Packing	#T1003 Credential Dumping	#T1082 System Information Discovery		#T1005 Data from Local System			
				#T1497 Virtualization/ Sandbox Evasion	#T1214 Credentials in Registry	#T1083 File and Directory Discovery					
						#T1012 Query Registry					
						#T1016 System Network Configuration Discovery					

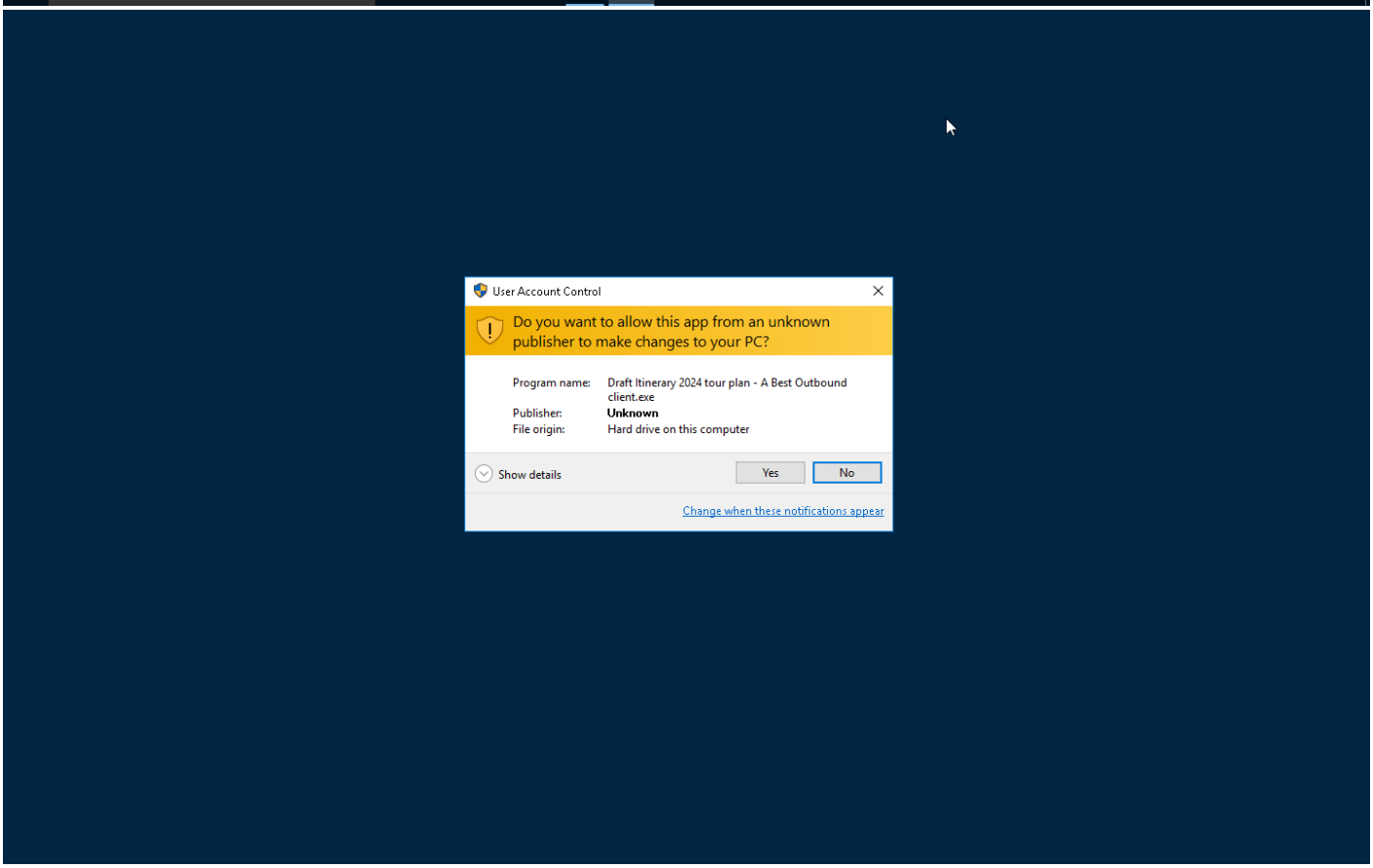
Sample Information

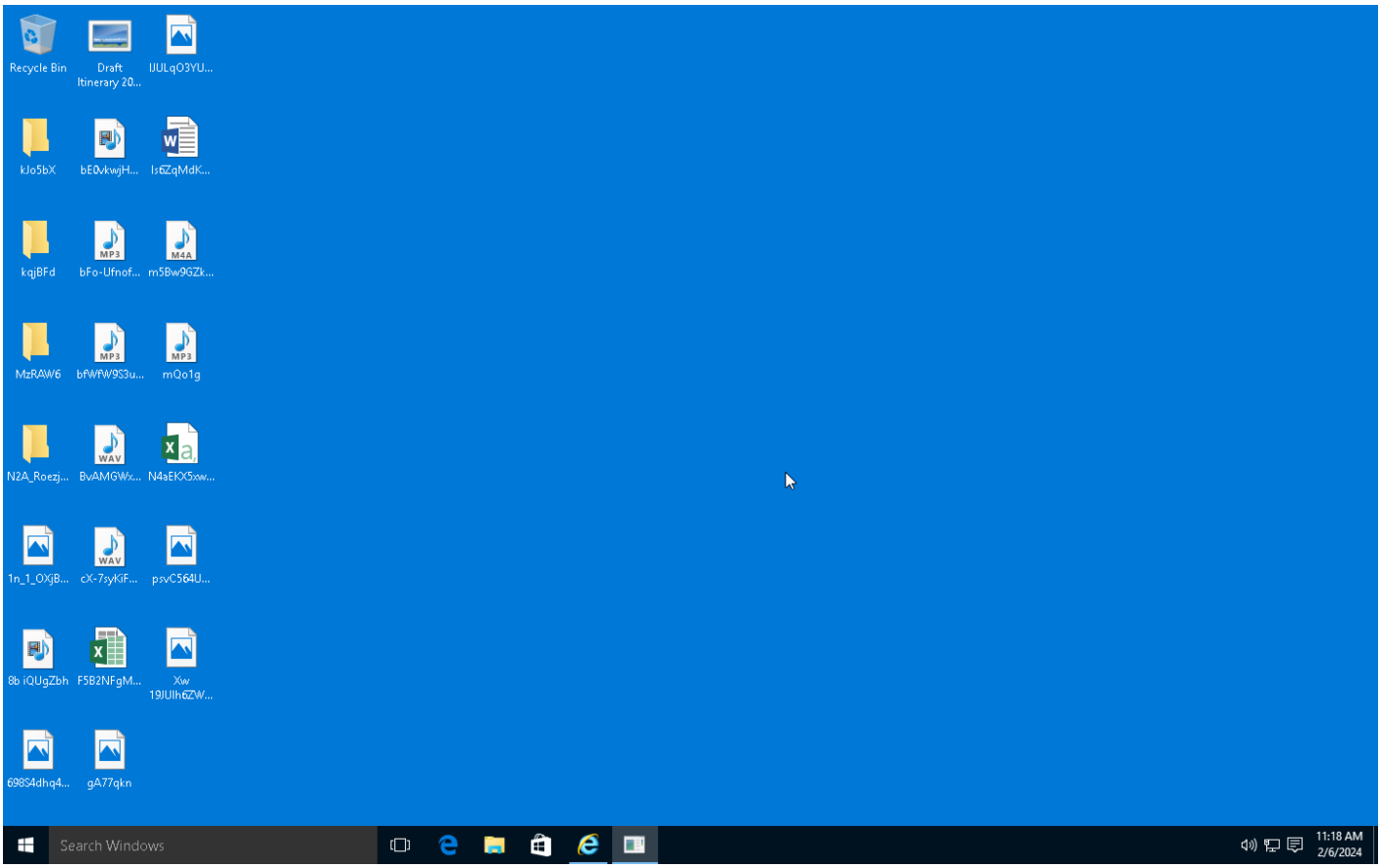
ID	#9819794
MD5	65bcf2c6ef1e115e4cc4e15e5a83bdfb
SHA1	e5830a23d3f18a44d99d34f1e8126283ab9a8caa
SHA256	ac71f9ab4ccb920a493508b0e0577b31fe547aa07e914f58f1def47d08ebcf7d
SSDeep	24576:HeQvWEQwYIFI8mZguwdH602ykWN2d+LuPE37oXMz:HeQvqwYIFB/lxCaPE38Xa
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	Draft Itinerary 2024 tour plan - A Best Outbound client.exe
File Size	1077.57 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

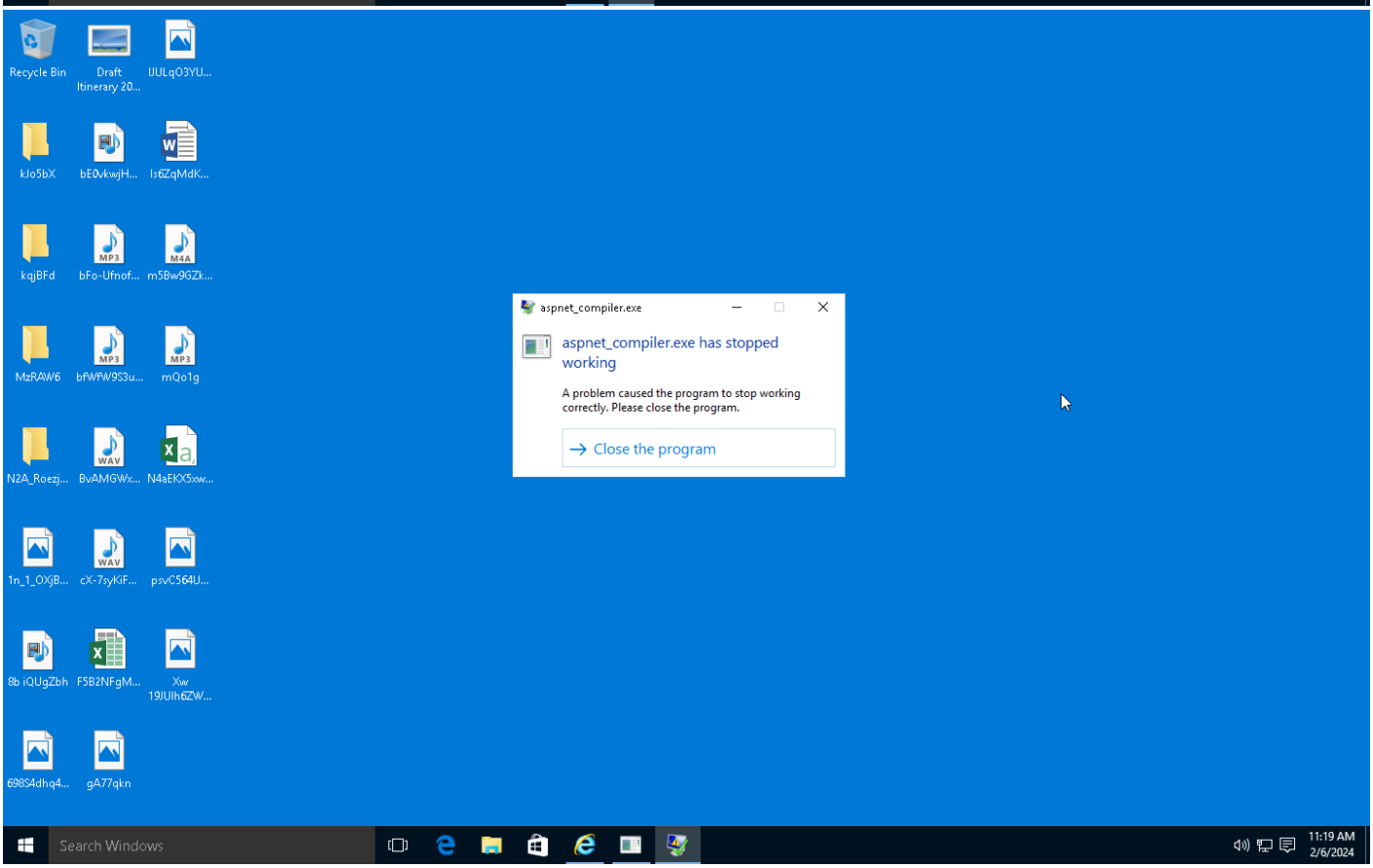
Analysis Information

Creation Time	2024-02-06 12:16 (UTC+1)
Analysis Duration	00:04:07
Termination Reason	Timeout
Number of Monitored Processes	6
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	1


Recycle Bin
Draft Itinerary 20...
IJULqO3YU...
kJo5bX
bE0vkwjH...
Is6ZqMdK...
kqjBFd
bFo-Ufnof...
m5Bw9GZk...
MzRAW6
bfWfW9S3u...
mQo1g
N2A_Roezj...
BvAMGWx...
N4sEKX5xw...
1n_1_OXjB...
cX-7syKiF...
psvC564U...
8b iQUgZbh
F5B2NFgM...
Xw 19IUIh6ZW...
698S4dhq4...
gA77qkn
Search Windows
11:18 AM
2/6/2024


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: Draft Itinerary 2024 tour plan - A Best Outbound client.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

2.67 KB total sent

5.29 KB total received

3 ports 80, 443, 53

3 contacted IP addresses

0 URLs extracted

3 files downloaded

1 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, 2.56 KB sent, 5.08 KB received

HTTP Requests

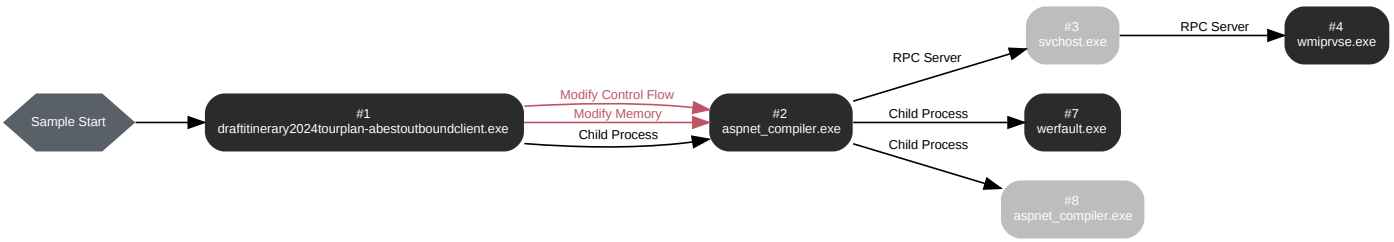
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://ip-api[.]com/line/?fields=hosting	-	-	-	0 bytes	CLEAN
POST	hxxps://discord[.]com/api/webhooks/1202330946817237022/1d5Ynow6yHbMqcRfr75qQjJVcSQnFlKpV4g5H2hHiKoRW33XeyZHnl-7hxdTf95oiy9f	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	discord[.]com	NO_ERROR	162.159.128.233, 162.159.138.232, 162.159.136.232, 162.159.137.232, 162.159.135.232	-	CLEAN
A	ip-api[.]com	NO_ERROR	208.95.112.1	-	CLEAN

BEHAVIOR

Process Graph



Process #1: draft itinerary 2024 tour plan - a best outbound client.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\draft itinerary 2024 tour plan - a best outbound client.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Draft Itinerary 2024 tour plan - A Best Outbound client.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 134787, Reason: Analysis Target
Unmonitor End Time	End Time: 145886, Reason: Terminated
Monitor duration	11.10s
Return Code	0
PID	4260
Parent PID	1656
Bitness	32 Bit

Host Behavior

Type	Count
Registry	1
File	6
Module	1
Process	1
-	3
-	7

Process #2: aspnet_compiler.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\aspnet_compiler.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 144044, Reason: Child Process
Unmonitor End Time	End Time: 177396, Reason: Crashed
Monitor duration	33.35s
Return Code	3762504530
PID	4844
Parent PID	4260
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\draft itinerary 2024 tour plan - a best outbound client.exe	0xd74	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\draft itinerary 2024 tour plan - a best outbound client.exe	0xd74	0x402000(4202496)	0x3b600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\draft itinerary 2024 tour plan - a best outbound client.exe	0xd74	0x43e000(4448256)	0x600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\draft itinerary 2024 tour plan - a best outbound client.exe	0xd74	0x440000(4456448)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\draft itinerary 2024 tour plan - a best outbound client.exe	0xd74	0x386008(3694600)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\draft itinerary 2024 tour plan - a best outbound client.exe	0xd74 / 0x12e4	0x43d51e(4445470)	-	✔	1

Host Behavior

Type	Count
-	37
Registry	71
File	43
User	4
Module	64
System	14
COM	56
Environment	11
-	1
-	2
-	6

Network Behavior

Type	Count
HTTP	1
HTTPS	1
DNS	2
TCP	2

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: 150202, Reason: RPC Server
Unmonitor End Time	End Time: 379604, Reason: Terminated by timeout
Monitor duration	229.40s
Return Code	Unknown
PID	1012
Parent PID	4844
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: 150202, Reason: RPC Server
Unmonitor End Time	End Time: 379604, Reason: Terminated by timeout
Monitor duration	229.40s
Return Code	Unknown
PID	4548
Parent PID	1012
Bitness	64 Bit

Host Behavior

Type	Count
System	16
Registry	6
Module	20
File	5
-	6

Process #7: werfault.exe

ID	7
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 4844 -s 1816
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 166166, Reason: Child Process
Unmonitor End Time	End Time: 177393, Reason: Terminated
Monitor duration	11.23s
Return Code	0
PID	5112
Parent PID	4844
Bitness	32 Bit

Host Behavior

Type	Count
Module	72
Environment	21
File	3
Registry	30

Process #8: aspnet_compiler.exe

ID	8
File Name	c:\windows\microsoft.net\framework\v4.0.30319\aspnet_compiler.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 166434, Reason: Child Process
Unmonitor End Time	End Time: 177152, Reason: Terminated
Monitor duration	10.72s
Return Code	259
PID	1908
Parent PID	4844
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ac71f9ab4ccb920a493508b0e0577b31fe547aa07e914f58f1def47d08ebcf7d	C:\Users\RDhJ0CNFevzX\Desktop\Draft Itinerary 2024 tour plan - A Best Outbound client.exe	Sample File	1077.57 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
527a8d47bb9dcdcc79b65ce54d6429a0294b1ea14768854db105db6ccd223edc	-	Memory Dump	264.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2ed27c1421e6928dbe13dbfdb5c59e1045b30341fe7ebe05700006bc5ac572c0	-	Downloaded File	6 bytes	text/plain	-	CLEAN
a1ade8321bec6b006f7bb387789eb89b90a51a1a0b2cb723f432a836a9810be0	-	Downloaded File	1.15 KB	text/plain	-	CLEAN
2d08a668532bcb703a130a12e07f30c1892633a6752e96c8eb0e9394dbf08da2	-	Downloaded File	45 bytes	application/json	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Draft Itinerary 2024 tour plan - A Best Outbound client.exe	Accessed File, Sample File	Access, Read	MALICIOUS
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe	Accessed File	Access	CLEAN
\\.\{017EF944-8C88-42C3-8F92-C8F7B6022F8D}	Accessed File	Access	CLEAN
\\.\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	Accessed File	Access	CLEAN
\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}	Accessed File	Access	CLEAN
\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	Accessed File	Access	CLEAN
\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\profiles.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\profiles.ini	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\Apple\Apple Application Support\plutil.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Storage\	Accessed File	Access	CLEAN
C:\mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files\Foxmail\mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\VirtualStore\Program Files (x86)\Foxmail\mail	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Mail\Opera Mail\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Mailbird\Store\Store.db	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WerFault.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://discord[.]com/api/webhooks/1202330946817237022/1d5Ynow6yHbMqcRfr75qQjJVcSQnFlKpV4g5H2hHiKoRW33XeyZHnl-7hxdTf95oiy9f	Extracted, Contacted	162.159.136.232, 162.159.128.233, 162.159.138.232, 162.159.135.232, 162.159.137.232	-	POST	MALICIOUS
hxxp://ip-api[.]com/line/?fields=hosting	Extracted, Contacted	208.95.112.1	United States	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
ip-api[.]com	208.95.112.1	United States	HTTP, DNS, TCP	CLEAN
discord[.]com	162.159.136.232, 162.159.128.233, 162.159.138.232, 162.159.135.232, 162.159.137.232	-	TCP, DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
162.159.128.233	discord[.]com	-	TCP, DNS, HTTPS	CLEAN
208.95.112.1	ip-api[.]com	United States	HTTP, DNS, TCP	CLEAN
162.159.138.232	discord[.]com	-	DNS	CLEAN
162.159.136.232	discord[.]com	-	DNS	CLEAN
162.159.137.232	discord[.]com	-	DNS	CLEAN
162.159.135.232	discord[.]com	-	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	aspnet_compiler.exe, draft itinerary 2024 tour plan - a best outbound client.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	aspnet_compiler.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	aspnet_compiler.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Profiles	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\Profiles	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Profiles	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	aspnet_compiler.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	access, read	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\ActiveSync\Partners	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreview	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1	access	aspnet_compiler.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework	access	werfault.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	werfault.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgDACSkipVerifyDlls	access, read	werfault.exe	CLEAN

Process

Process Name	Commandline	Verdict
draft itinerary 2024 tour plan - a best outbound client.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Draft Itinerary 2024 tour plan - A Best Outbound client.exe"	MALICIOUS
aspnet_compiler.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
aspnet_compiler.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"	CLEAN
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 4844 -s 1816	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_HTML_Message	Agent Tesla html-formatted message	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
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	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	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

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