MALICIOUS

Classifications: Backdoor

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**f364d1b15bb2049549d9084496ad239b.exe**
ID	#9997342
MD5	f364d1b15bb2049549d9084496ad239b
SHA1	adbe8eb29c5e442a8515ba9c63a62126427ada8e
SHA256	e846d3cfad85b09f8fdb0460fff53cfda1176f4e9e420bf60ed88d39b1ef93db
File Size	4905.00 KB
Report Created	2024-03-04 19:00 (UTC+1)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 35 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 debugger	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe tries to detect a debugger via API "IsDebuggerPresent".			
2/5	Discovery	Collects hardware properties	2	-
	• (Process #3) wmic.exe queries hardware properties via WMI: SELECT Name FROM WIN32_PROCESSOR. • (Process #7) wmic.exe queries hardware properties via WMI: SELECT Name FROM win32_VideoController.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe reads the network adapters' addresses by API.			
2/5	Discovery	Searches for sensitive browser data	13	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Amigo" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Torch" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Uran" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Chrome Canary" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "7Star" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe searches for sensitive data of web browser "Kometa" by file.			
2/5	Network Connection	Sets up server that accepts incoming connections	3	Backdoor
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe starts a TCP server listening on port 49696. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe starts a TCP server listening on port 49694. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe starts a TCP server listening on port 49697.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Reads system data	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe reads the cryptographic machine GUID from registry.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe starts (process #3) wmic.exe with a hidden window. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe starts (process #7) wmic.exe with a hidden window.			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #1) f364d1b15bb2049549d9084496ad239b.exe tries to gather information about application "FileZilla" by file.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe enumerates running processes.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe resolves hostname "ipinfo.io" to IP "34.117.186.192".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe opens an outgoing TCP connection to host "193.178.170.30:80". • (Process #1) f364d1b15bb2049549d9084496ad239b.exe opens an outgoing TCP connection to host "34.117.186.192:80".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.exe resolves 255 API functions by name.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #1) f364d1b15bb2049549d9084496ad239b.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

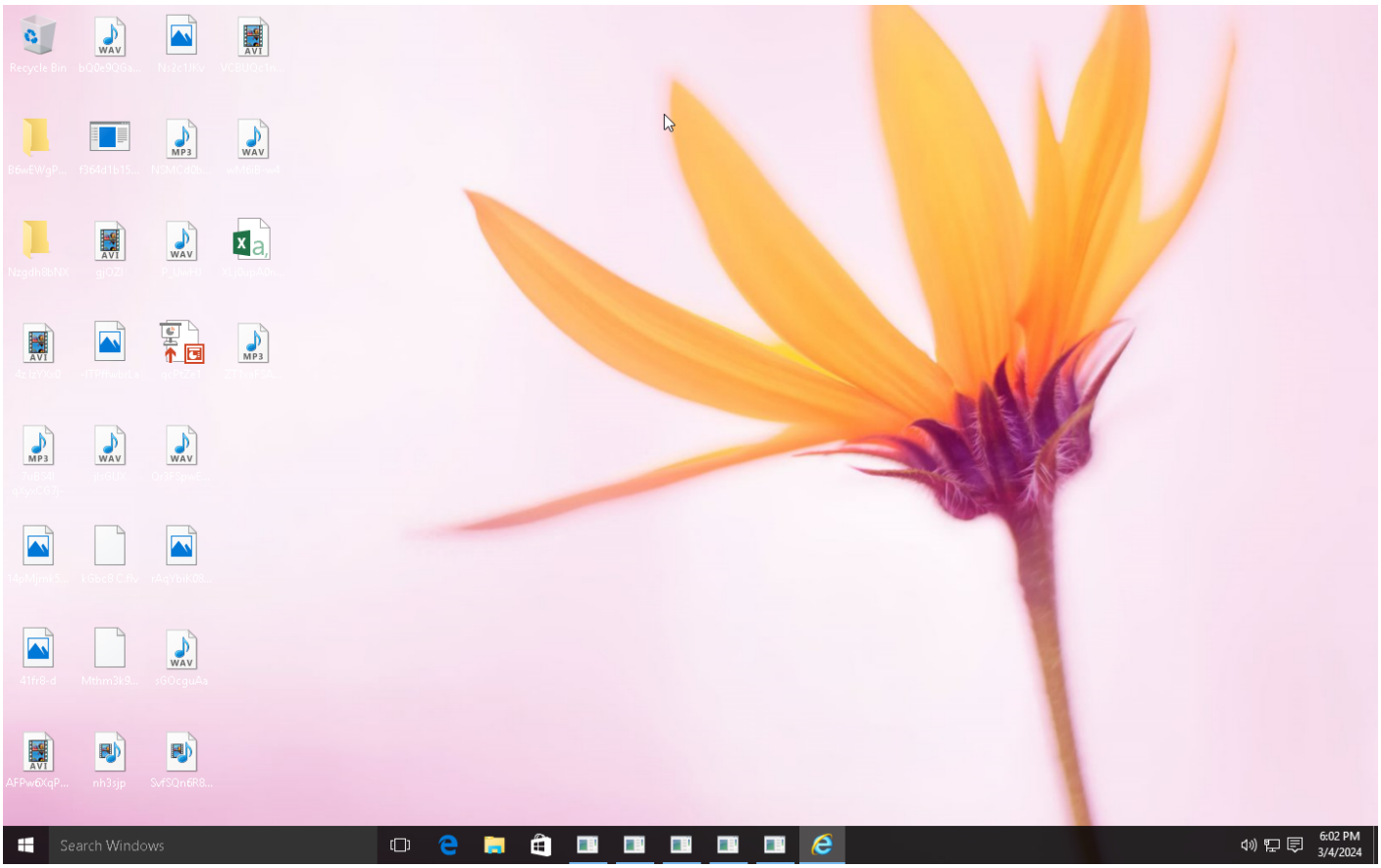
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery	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

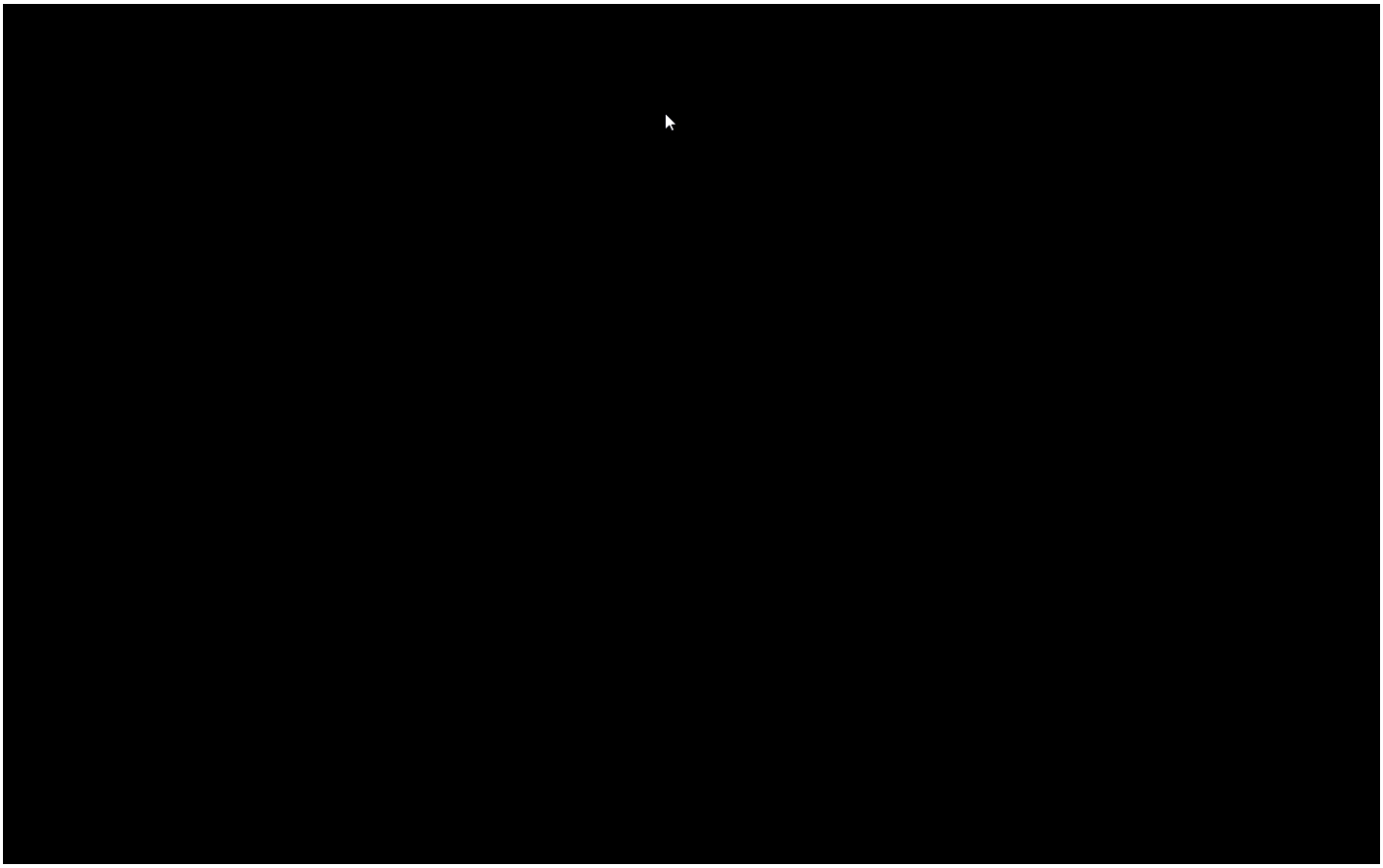
Sample Information

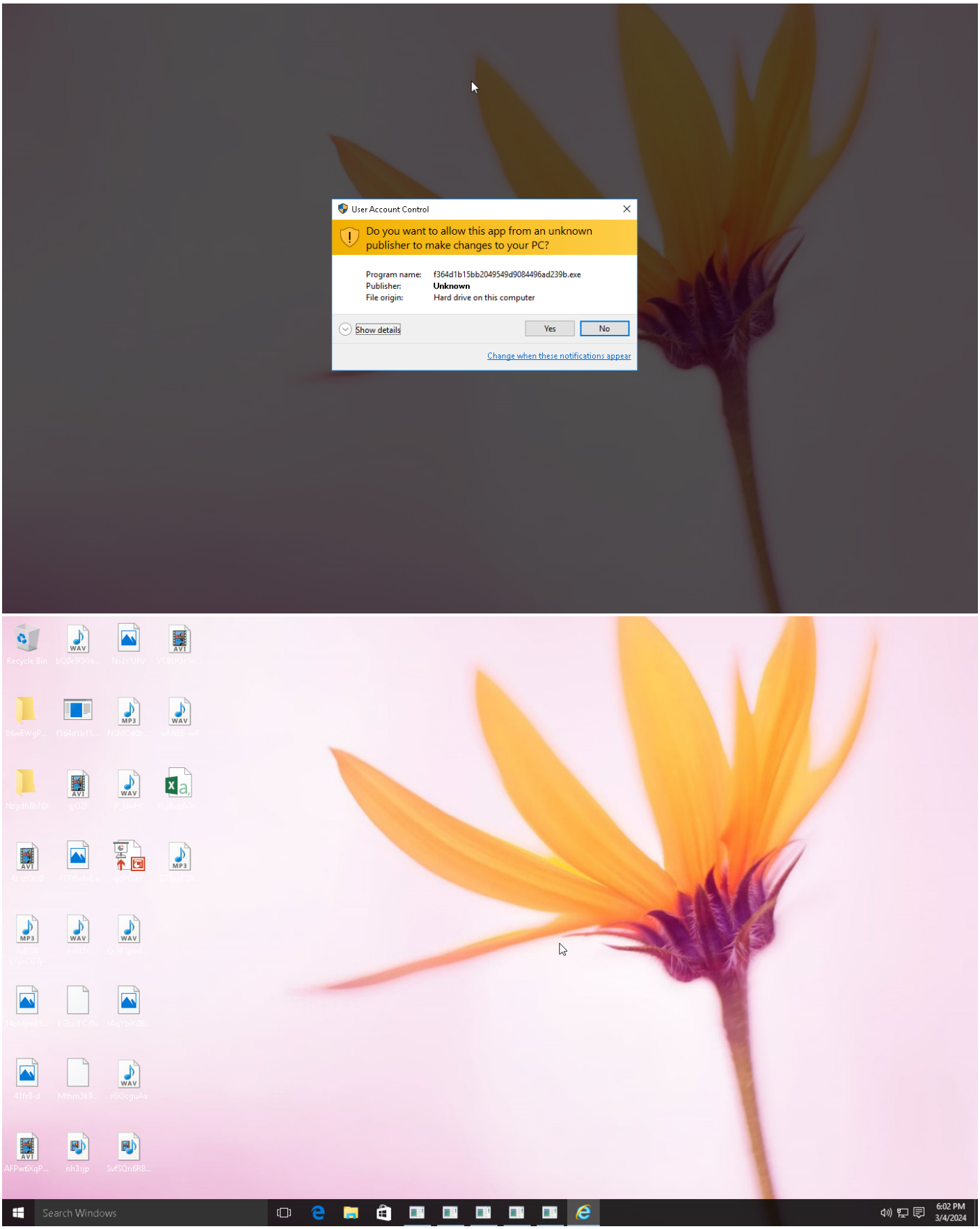
ID	#9997342
MD5	f364d1b15bb2049549d9084496ad239b
SHA1	adbe8eb29c5e442a8515ba9c63a62126427ada8e
SHA256	e846d3cfad85b09f8fdb0460fff53cfda1176f4e9e420bf60ed88d39b1ef93db
SSDeep	98304:GL4AFoEMQEbPjwV/xQzp2FMhsTBfkIS2oFw5gmpp4k:26EMnb7kZw4FMaTRkItym
ImpHash	9aebf3da4677af9275c461261e5abde3
File Name	f364d1b15bb2049549d9084496ad239b.exe
File Size	4905.00 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2024-03-04 19:00 (UTC+1)
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


Search Windows
6:02 PM
3/4/2024





Screenshots truncated

NETWORK

General

2.53 KB total sent

1.68 KB total received

2 ports 80, 53

3 contacted IP addresses

0 URLs extracted

5 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

3 URLs contacted, 2 servers

3 sessions, 2.48 KB sent, 1.61 KB received

HTTP Requests

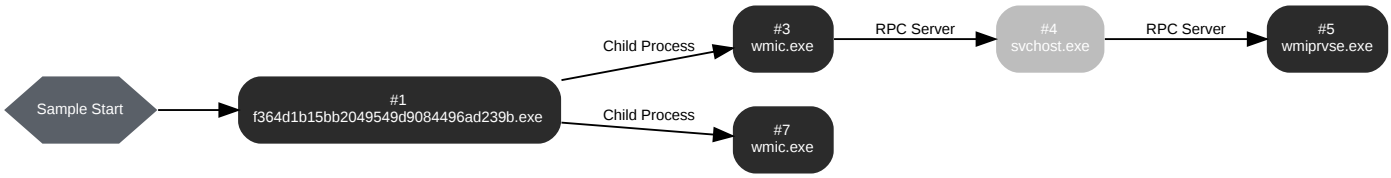
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://ipinfo[.]io	-	-	-	0 bytes	CLEAN
POST	hxxp://193[.]178[.]170[.]30/submit/info	-	-	-	0 bytes	CLEAN
POST	hxxp://193[.]178[.]170[.]30/submit/file	-	-	-	0 bytes	CLEAN

DNS Requests

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

BEHAVIOR

Process Graph



Process #1: f364d1b15bb2049549d9084496ad239b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\f364d1b15bb2049549d9084496ad239b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f364d1b15bb2049549d9084496ad239b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 128268, Reason: Analysis Target
Unmonitor End Time	End Time: 229557, Reason: Terminated
Monitor duration	101.29s
Return Code	0
PID	4468
Parent PID	-
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\os6nBSYL.zip	446 bytes	a31ad03b83f0aa4e4eb8372b46c25c46f2d217de855b1a3cd388a38806c35447	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\system.txt	535 bytes	4d064bae23085e238a30783829220be9f90e6886856633f5e43e525787157ec9	✖

Host Behavior

Type	Count
Module	300
System	26
Environment	73
-	13
File	384
User	2
-	1
Registry	8
-	8
Process	109
-	1

Network Behavior

Type	Count
HTTP	3
DNS	1
TCP	3

Process #3: wmic.exe

ID	3
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic cpu get name
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 171389, Reason: Child Process
Unmonitor End Time	End Time: 176569, Reason: Terminated
Monitor duration	5.18s
Return Code	0
PID	5016
Parent PID	4468
Bitness	64 Bit

Host Behavior

Type	Count
Module	10
COM	9
System	7
Registry	5
File	8
-	1

Process #4: svchost.exe

ID	4
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: 172538, Reason: RPC Server
Unmonitor End Time	End Time: 369944, Reason: Terminated by timeout
Monitor duration	197.41s
Return Code	Unknown
PID	1012
Parent PID	5016
Bitness	64 Bit

Process #5: wmiprvse.exe

ID	5
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: 172539, Reason: RPC Server
Unmonitor End Time	End Time: 369944, Reason: Terminated by timeout
Monitor duration	197.41s
Return Code	Unknown
PID	4460
Parent PID	1012
Bitness	64 Bit

Host Behavior

Type	Count
System	7

Process #7: wmic.exe

ID	7
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic path win32_VideoController get name
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178721, Reason: Child Process
Unmonitor End Time	End Time: 182053, Reason: Terminated
Monitor duration	3.33s
Return Code	0
PID	4808
Parent PID	4468
Bitness	64 Bit

Host Behavior

Type	Count
Module	10
COM	9
System	7
Registry	5
File	8
-	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e846d3cfad85b09f8fdb0460ff f53cfda1176f4e9e420bf60ed 88d39b1ef93db	C: \Users\RDhJ0CNFevzX\Desktop\f364 d1b15bb2049549d9084496ad239b.exe	Sample File	4905.00 KB	application/ vnd.microsoft.portable-executable	-	MALICIOUS
a99a755129d0d6cca666ccc 51c6df69f77ee5292a9588e4 8702184bd23234eff	-	Downloaded File	312 bytes	application/json	-	CLEAN
966a3882930698ad2c64ee8f 3a296458406f97c46815555d dd91a5b9182300fac	-	Downloaded File	524 bytes	application/json	-	CLEAN
84da13f8b72911e62aaead5a f60e91beee6af925c7f926f3d 426b6f7bc346619	-	Downloaded File	66 bytes	application/json	-	CLEAN
a31ad03b83f0aa4e4eb8372b 46c25c46f2d217de855b1a3c d388a38806c35447	C: \Users\RDHJ0C~1\AppData\Local\Te mp\os6nBSYL.zip, C:\\Users\ \RDHJ0C~1\\AppData\\Local\\Temp\ \os6nBSYL-46246cf2-4ef3-491d-866c-5 d417187d893.zip, C: \Users\RDHJ0C~1\AppData\Local\Te mp\os6nBSYL-46246cf2-4ef3-491d-86 6c-5d417187d893.zip	Downloaded File	446 bytes	application/zip	Access, Create, Delete, Read, Write	CLEAN
c955e57777ec0d73639dca6 748560d00aa5eb8e12f13ebb 2ed9656add3908f97	-	Downloaded File	16 bytes	application/json	-	CLEAN
4d064bae23085e238a30783 829220be9f90e6886856633f 5e43e525787157ec9	system.txt, C: \Users\RDHJ0C~1\AppData\Local\Te mp\system.txt	Archive File	535 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C: \Users\RDhJ0CNFevzX\Desktop\f364d1b15bb2049549d9084496ad23 9b.exe	Sample File	-	MALICIOUS
C:\\Users\\RDHJ0C~1\\AppData\\Local\\Temp\ \os6nBSYL-46246cf2-4ef3-491d-866c-5d417187d893.zip	Downloaded File	-	CLEAN
system.txt	Miscellaneous File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\system.txt	Accessed File, Dropped File, Extracted File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\os6nBSYL.zip	Accessed File, Downloaded File, Extracted File	Access, Create, Delete, Write	CLEAN
C: \Users\RDHJ0C~1\AppData\Local\Temp\os6nBSYL-46246cf2-4ef3-49 1d-866c-5d417187d893.zip	Accessed File, Downloaded File, Extracted File	Access, Read	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

File Name	Category	Operations	Verdict
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
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

File Name	Category	Operations	Verdict
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\RDHJ0C~1\AppData\Local\Temp\Cookies	Accessed File	Access, Create, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome SxS\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome SxS\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Local State	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming/discord/Local Storage/leveldb/	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming/discord/Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming/discordptb/Local Storage/leveldb/	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming/discordptb/Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming/discordcanary/Local Storage/leveldb/	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming/discordcanary/Local State	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\exodus	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Exodus	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coinomi	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Monero	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\atomic	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Electrum	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\autofills.txt	Accessed File	Access, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\passwords.txt	Accessed File	Access, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\bookmarks.txt	Accessed File	Access, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\cards.txt	Accessed File	Access, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\discord-tokens.txt	Accessed File	Access, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\exodus-passwords.txt	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\intentlauncher\launcherconfig	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\.lunarclient\settings\game\accounts.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.minecraft\TlauncherProfiles.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.feather\accounts.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.minecraft\meteor-client\accounts.nbt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.minecraft\Impact\alts.json	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.minecraft\Novoline\alts.novo	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.minecraft\launcher_accounts_microsoft_store.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.minecraft\Rise\alts.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\intentlauncher\Rise\alts.txt	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\paladium-group\accounts.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\PolyMC\accounts.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Badlion Client\accounts.json	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Exodus\exodus.wallet	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\coinomi\coinomi\wallets	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Tox	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Monero\wallets	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\atomic\databases	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Electrum\wallets	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Telegram Desktop\tdata	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Signal	Accessed File	Access	CLEAN
C:\Program Files (x86)\Steam\config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://ipinfo[.]io	Contacted, Extracted	34.117.186.192	United States	GET	CLEAN
hxxp://193[.]178[.]170[.]30/submit/info	Contacted, Extracted	193.178.170.30	Russia	POST	CLEAN
hxxp://193[.]178[.]170[.]30/submit/file	Contacted, Extracted	193.178.170.30	Russia	POST	CLEAN

Domain

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

IP

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

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	f364d1b15bb2049549d9084496ad239b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	f364d1b15bb2049549d9084496ad239b.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	f364d1b15bb2049549d9084496ad239b.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	f364d1b15bb2049549d9084496ad239b.exe	CLEAN
HKEY_CURRENT_USER\Software\iPwonTCGCC	create, access	f364d1b15bb2049549d9084496ad239b.exe	CLEAN
HKEY_CURRENT_USER\Software\iPwonTCGCC\ID	access, write	f364d1b15bb2049549d9084496ad239b.exe	CLEAN

Process

Process Name	Commandline	Verdict
f364d1b15bb2049549d9084496ad239b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\f364d1b15bb2049549d9084496ad239b.exe"	MALICIOUS
wmic.exe	wmic cpu get name	SUSPICIOUS
wmic.exe	wmic path win32_VideoController get name	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

No YARA or AV matches available.

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	2024.1.2
Dynamic Engine Version	2024.1.2 / 02/16/2024 05:23
Static Engine Version	2024.1.2.0 / 2024-02-16 04:00:11
AV Exceptions Version	2024.1.2.24 / 2024-02-12 14:04:13
Link Detonation Heuristics Version	2024.1.2.30 / 2024-02-29 15:50:18
Smart Memory Dumping Rules Version	2024.1.2.30 / 2024-02-29 15:50:18
Config Extractors Version	2024.1.2.30 / 2024-02-29 15:50:18
Signature Trust Store Version	2024.1.2.24 / 2024-02-12 14:04:13
VMRay Threat Identifiers Version	2024.1.2.31 / 2024-03-04 09:31:25
YARA Built-in Ruleset Version	2024.1.2.30

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