MALICIOUS

Classifications: Backdoor

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**83741e7578d11053fd5cbbf15ed253b3.exe**
ID	#9878844
MD5	83741e7578d11053fd5cbbf15ed253b3
SHA1	e95948bdfcf0355afc81e913caeb319b7fb1318c
SHA256	beb1e444d4a7e27ca6cb5fe55e9eaa3ecf880c044755d72f7724e7fea8371cd5
File Size	4268.50 KB
Report Created	2024-02-13 20:59 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 40 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.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.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) 83741e7578d11053fd5cbbf15ed253b3.exe has a thread which sleeps more than 5 minutes.			
2/5	Discovery	Searches for sensitive browser data	13	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Google Chrome" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Amigo" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Torch" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Yandex Browser" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Uran" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Chrome Canary" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Vivaldi" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Sputnik" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "7Star" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "CentBrowser" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Orbitum" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe searches for sensitive data of web browser "Kometa" by file.			
2/5	Network Connection	Sets up server that accepts incoming connections	9	Backdoor
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49165. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49169. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49168. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49166. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49170. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49163. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49167. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49164. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts a TCP server listening on port 49162.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe enumerates running processes.			
1/5	Discovery	Reads system data	1	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe reads the cryptographic machine GUID from registry.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts (process #2) wmic.exe with a hidden window. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe starts (process #6) wmic.exe with a hidden window.			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe tries to gather information about application "FileZilla" by file.			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe resolves hostname "hzp02itt0a.com" to IP "193.178.170.30". • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe resolves hostname "ipinfo.io" to IP "34.117.186.192".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe opens an outgoing TCP connection to host "193.178.170.30:80". • (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe opens an outgoing TCP connection to host "34.117.186.192:80".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.exe resolves 253 API functions by name.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #1) 83741e7578d11053fd5cbbf15ed253b3.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					

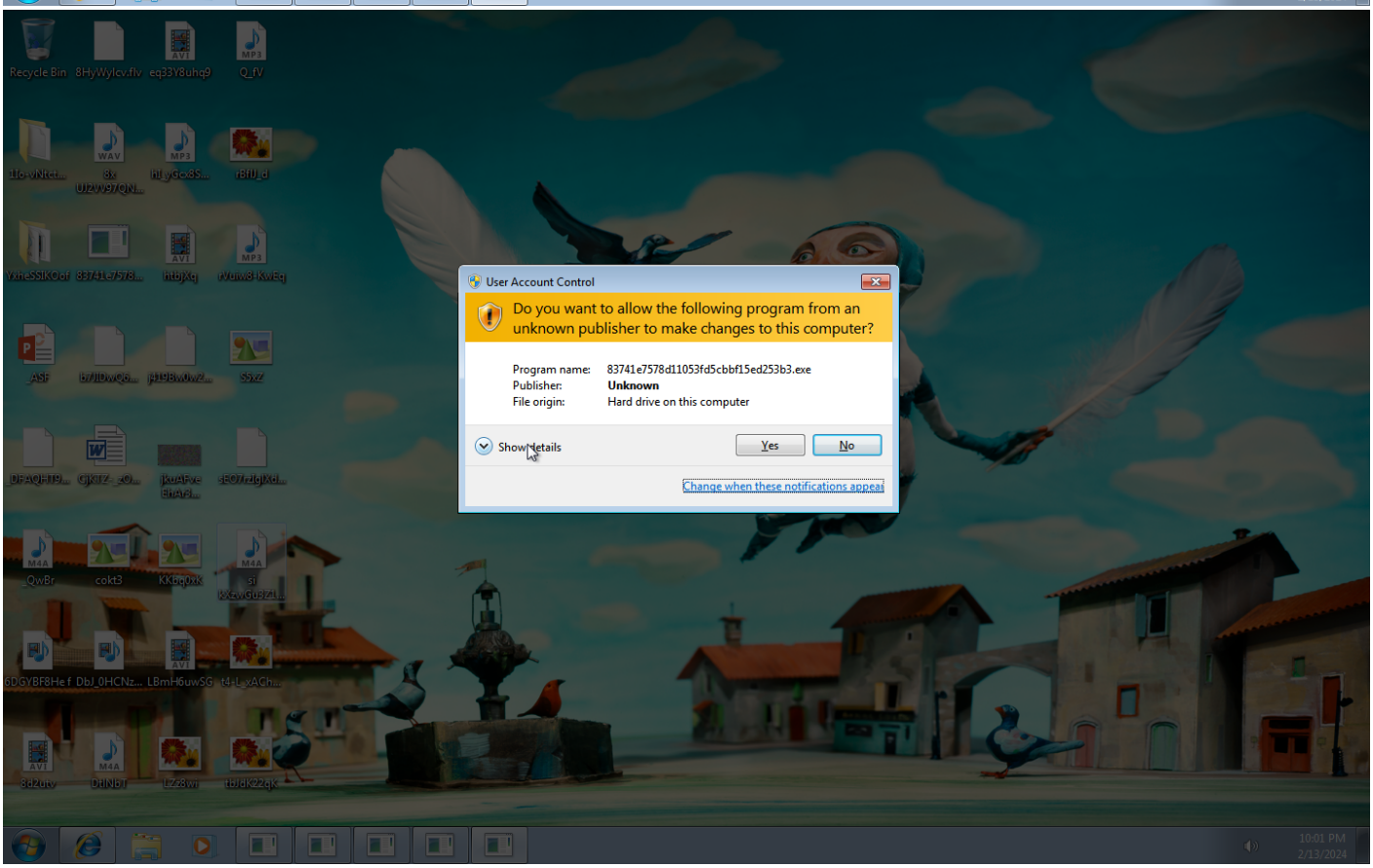
Sample Information

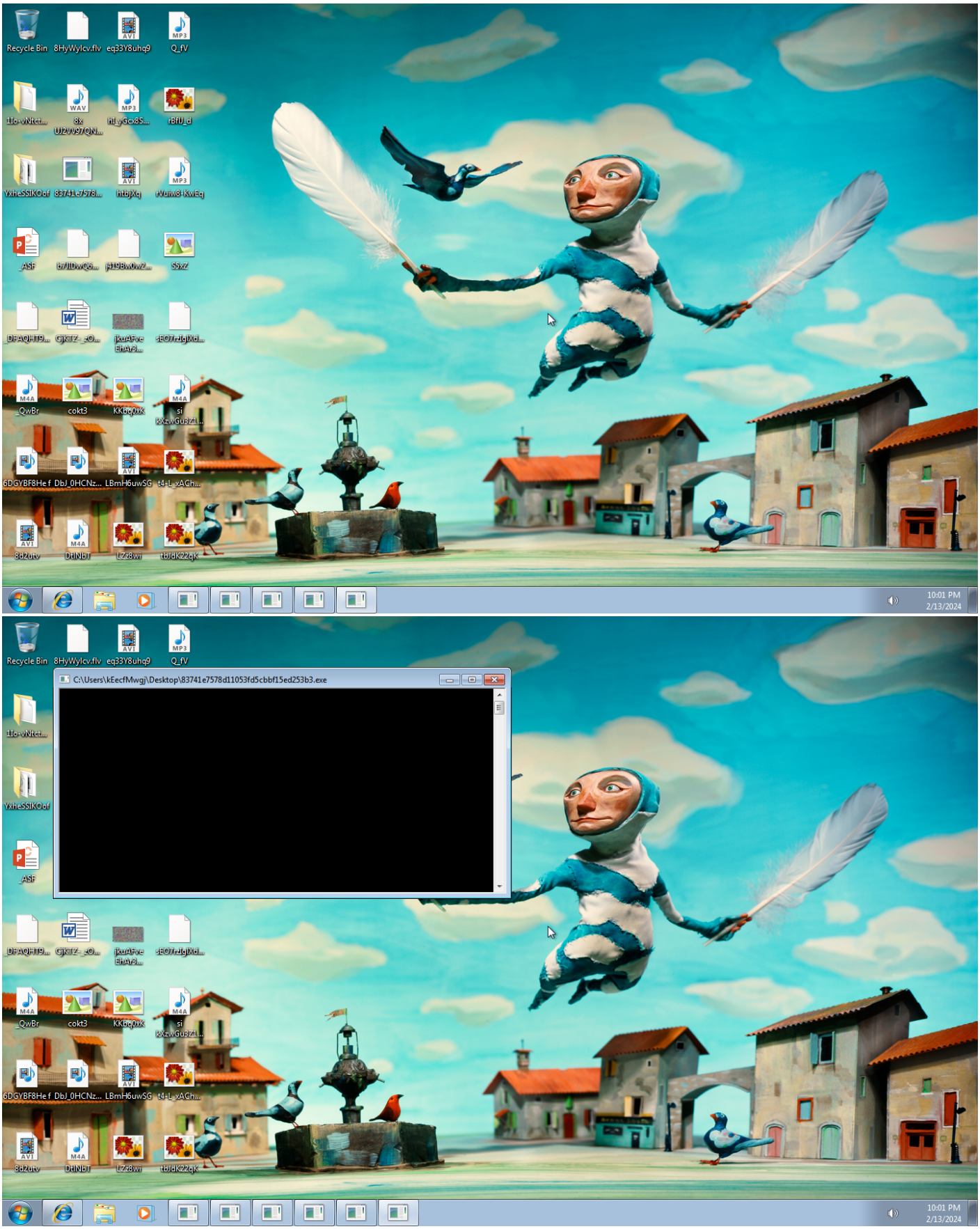
ID	#9878844
MD5	83741e7578d11053fd5cbbf15ed253b3
SHA1	e95948bdfcf0355afc81e913caeb319b7fb1318c
SHA256	beb1e444d4a7e27ca6cb5fe55e9eaa3ecf880c044755d72f7724e7fea8371cd5
SSDeep	98304:x4RhOygpdPL0UH+TI8zm/tlF2lREpF9MBeE7eUxhx1u:uRhDw+IWQtD2ldJG
ImpHash	9aebf3da4677af9275c461261e5abde3
File Name	83741e7578d11053fd5cbbf15ed253b3.exe
File Size	4268.50 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2024-02-13 20:59 (UTC)
Analysis Duration	00:03:52
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


Recycle Bin
8HyWylcv.flv
eq33Y8uhq9
Q_fV
_QwBr
cokt3
si
6DGYBF8Hef
DbJ_0HCNz...
LBmH6uwSG
t4-L_xACh...
8d2utv
DHNBT
LZz8.wi
tbJdK22qk
10:01 PM
2/13/2024


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 83741e7578d11053fd5cbbf15ed253b3.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

5.80 KB total sent

5.50 KB total received

2 ports 80, 53

3 contacted IP addresses

0 URLs extracted

11 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

3 URLs contacted, 2 servers

9 sessions, 5.69 KB sent, 5.36 KB received

HTTP Requests

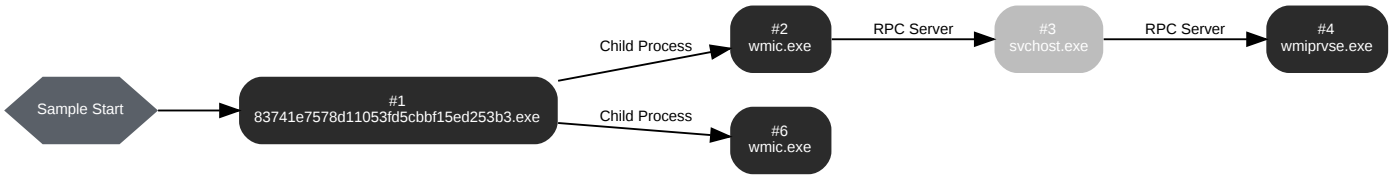
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://hzp02itt0a[.]com/submit/error	-	-	-	0 bytes	CLEAN
GET	hxxp://ipinfo[.]io	-	-	-	0 bytes	CLEAN
POST	hxxp://193[.]178[.]170[.]30/submit/info	-	-	-	0 bytes	CLEAN

DNS Requests

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

BEHAVIOR

Process Graph



Process #1: 83741e7578d11053fd5cbbf15ed253b3.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\83741e7578d11053fd5cbbf15ed253b3.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\83741e7578d11053fd5cbbf15ed253b3.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89329, Reason: Analysis Target
Unmonitor End Time	End Time: 179925, Reason: Terminated
Monitor duration	90.60s
Return Code	0
PID	3940
Parent PID	1912
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\zTmOZs75.zip	443 bytes	8aade8e26fc302b5381d0dc5a87a6e48b55de08ef9f8d2dd4f534757927aa2b8	✖
C:\Users\KEECFM~1\AppData\Local\Temp\system.txt	542 bytes	93e602b729a215adc44335bed89dd55d82f7d0d3c243a6fd8b53aa8e2cc94498	✖

Host Behavior

Type	Count
Module	307
System	31
Environment	76
-	13
File	385
User	2
Process	878
Registry	8
-	8
-	8

Network Behavior

Type	Count
HTTP	9
DNS	2
TCP	9

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: 145808, Reason: Child Process
Unmonitor End Time	End Time: 151102, Reason: Terminated
Monitor duration	5.29s
Return Code	0
PID	4024
Parent PID	3940
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: 147823, Reason: RPC Server
Unmonitor End Time	End Time: 322092, Reason: Terminated by timeout
Monitor duration	174.27s
Return Code	Unknown
PID	876
Parent PID	4024
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: 147823, Reason: RPC Server
Unmonitor End Time	End Time: 322092, Reason: Terminated by timeout
Monitor duration	174.27s
Return Code	Unknown
PID	3332
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: 149902, Reason: Child Process
Unmonitor End Time	End Time: 154139, Reason: Terminated
Monitor duration	4.24s
Return Code	0
PID	4056
Parent PID	3940
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
beb1e444d4a7e27ca6cb5fe55e9eaa3ecf880c044755d72f7724e7fea8371cd5	C:\Users\kEecfMwgj\Desktop\83741e7578d11053fd5cbbf15ed253b3.exe	Sample File	4268.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
02f37f485cfe3f36477c15d029c0628860486227b23e33befed306d302353124	-	Downloaded File	313 bytes	application/json	-	CLEAN
534f40067436a35d1f9b71b6a5c40d5274588967e6edaeda6bd7b9be19d8dc17	-	Downloaded File	177 bytes	application/json	-	CLEAN
c955e57777ec0d73639dca6748560d00aa5eb8e12f13ebb2ed9656add3908f97	-	Downloaded File	16 bytes	application/json	-	CLEAN
9651e33df1b7b22f0dc0990778a4cdcb263471968a72db27dac07867c7d13d00	-	Downloaded File	177 bytes	application/json	-	CLEAN
00da859b1a29d0428acd3a560e736bffc6b49d8002badc3947f2616da768353f	-	Downloaded File	177 bytes	application/json	-	CLEAN
b42fbaba331fe0d4db4179ac4b596ea0a3e4df58cb1225f9dffe8eaacb49f892	-	Downloaded File	173 bytes	application/json	-	CLEAN
b6c9a83b72bff4e5f2b419f48f86abdd6f862f962385bfe67ee62e53ae083608	-	Downloaded File	182 bytes	application/json	-	CLEAN
41574f1b81210bbe34bd40d6639cffbd29284f21f9c11fe729dad7df069909c4	-	Downloaded File	184 bytes	application/json	-	CLEAN
17eb6a2db6a8f5c8db878efb9c13ad022f3059f2d95291d471c35a314fbfcb62	-	Downloaded File	66 bytes	application/json	-	CLEAN
5a12da61bd2003783ac3ce61601020101bb55139664141b171e1030a96e44e34	-	Downloaded File	1.10 KB	application/json	-	CLEAN
74234e98afe7498fb5daf1f36ac2d78acc339464f950703b8c019892f982b90b	-	Downloaded File	4 bytes	text/plain	-	CLEAN
93e602b729a215adc44335bed89dd55d82f7d0d3c243a6fd8b53aa8e2cc94498	system.txt, C:\Users\KEECFM~1\AppData\Local\Temp\system.txt	Archive File	542 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
8aade8e26fc302b5381d0dc5a87a6e48b55de08ef9f8d2dd4f534757927aa2b8	C:\Users\KEECFM~1\AppData\Local\Temp\zTmOZs75.zip	Dropped File	443 bytes	application/zip	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\83741e7578d11053fd5cbbf15ed253b3.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\zTmOZs75.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

File Name	Category	Operations	Verdict
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
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

File Name	Category	Operations	Verdict
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
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

File Name	Category	Operations	Verdict
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
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\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

File Name	Category	Operations	Verdict
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
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
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

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/error	Extracted, Contacted	193.178.170.30	Russia	POST	CLEAN
hxxp://193[.]178[.]170[.]30/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, DNS, TCP	CLEAN
hzp02itt0a[.]com	193.178.170.30	Russia	HTTP, DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
193.178.170.30	hzp02itt0a[.]com	Russia	HTTP, DNS, 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	83741e7578d11053fd5cbbf15ed253b3.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	83741e7578d11053fd5cbbf15ed253b3.exe	CLEAN
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	83741e7578d11053fd5cbbf15ed253b3.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	83741e7578d11053fd5cbbf15ed253b3.exe	CLEAN
HKEY_CURRENT_USER\Software\iPwonTCGCC	create, access	83741e7578d11053fd5cbbf15ed253b3.exe	CLEAN
HKEY_CURRENT_USER\Software\iPwonTCGCC\ID	write, access	83741e7578d11053fd5cbbf15ed253b3.exe	CLEAN

Process

Process Name	Commandline	Verdict
83741e7578d11053fd5cbbf15ed253b3.exe	"C:\Users\kEecfMwgj\Desktop\83741e7578d11053fd5cbbf15ed253b3.exe"	MALICIOUS
wmic.exe	wmic cpu get name	SUSPICIOUS
wmic.exe	wmic path win32_VideoController get name	SUSPICIOUS
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