MALICIOUS

Classifications: Downloader | Injector

Threat Names: SmokeLoader | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe**
ID	#3231310
MD5	dc67c627917ff9724f3c1e6db5f2dc27
SHA1	4b7528999ad6095b3fbb3aec059efb88d999ea95
SHA256	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da
File Size	335.00 KB
Report Created	2022-01-04 20:55 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (20 rules, 26 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe. • Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe creates thread in (process #3) explorer.exe.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "host-data-coin-11.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih". • (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #6) 506a.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe modifies memory of (process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe alters context of (process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Logon. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Time. Task has been rescheduled by the analyzer.			
1/5	Obfuscation	Reads from memory of another process	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe reads from (process #2) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #3) explorer.exe enumerates running processes.			
1/5	Mutex	Creates mutex	1	-
	• (Process #3) explorer.exe creates mutex with name "FE7F15060B875FB9FB2A49F08D5D03120C287F38".			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe resolves 41 API functions by name. • (Process #6) 506a.exe resolves 44 API functions by name.			
1/5	Network Connection	Downloads executable	1	Downloader
	• (Process #3) explorer.exe downloads executable via http from 185.206.212.165/build_dl.			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #3) explorer.exe tries to connect to TCP port 20000 at 185.206.212.165.			
1/5	Execution	Executes itself	2	-
	• (Process #1) 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe. • (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe.			

Mitre ATT&CK Matrix

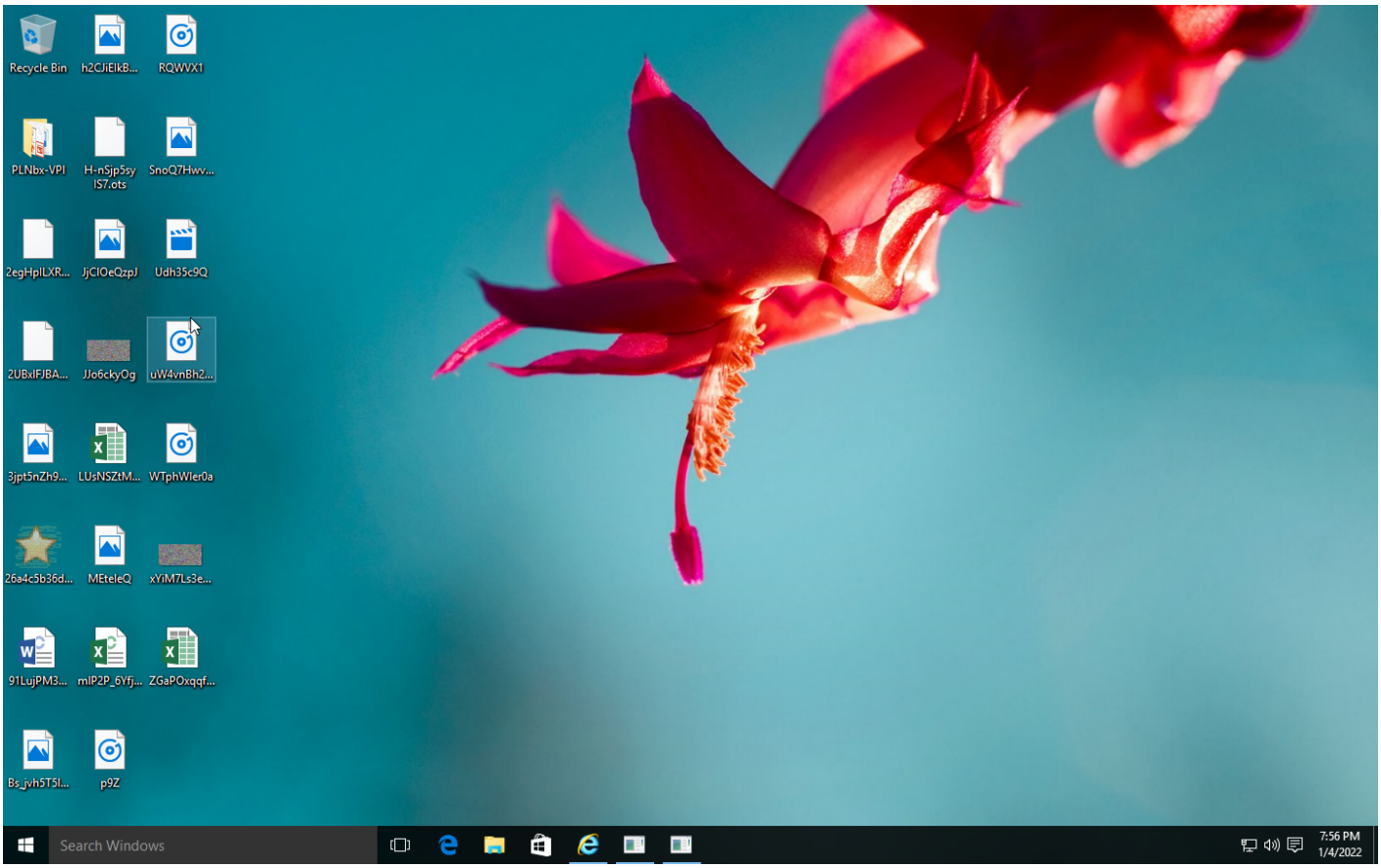
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
				#T1096 NTFS File Attributes		#T1497 Virtualization/ Sandbox Evasion			#T1105 Remote File Copy		
				#T1497 Virtualization/ Sandbox Evasion					#T1065 Uncommonly Used Port		

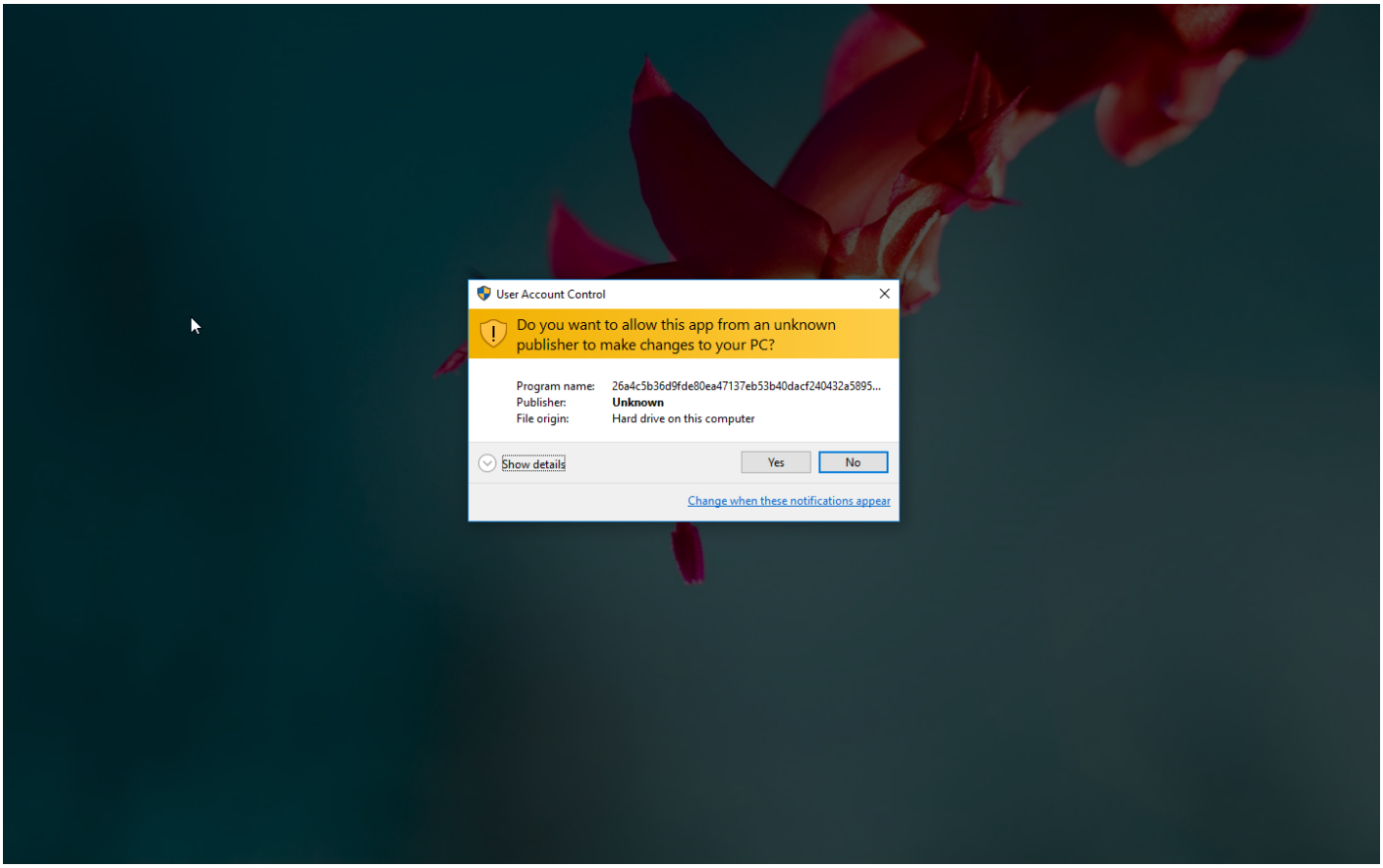
Sample Information

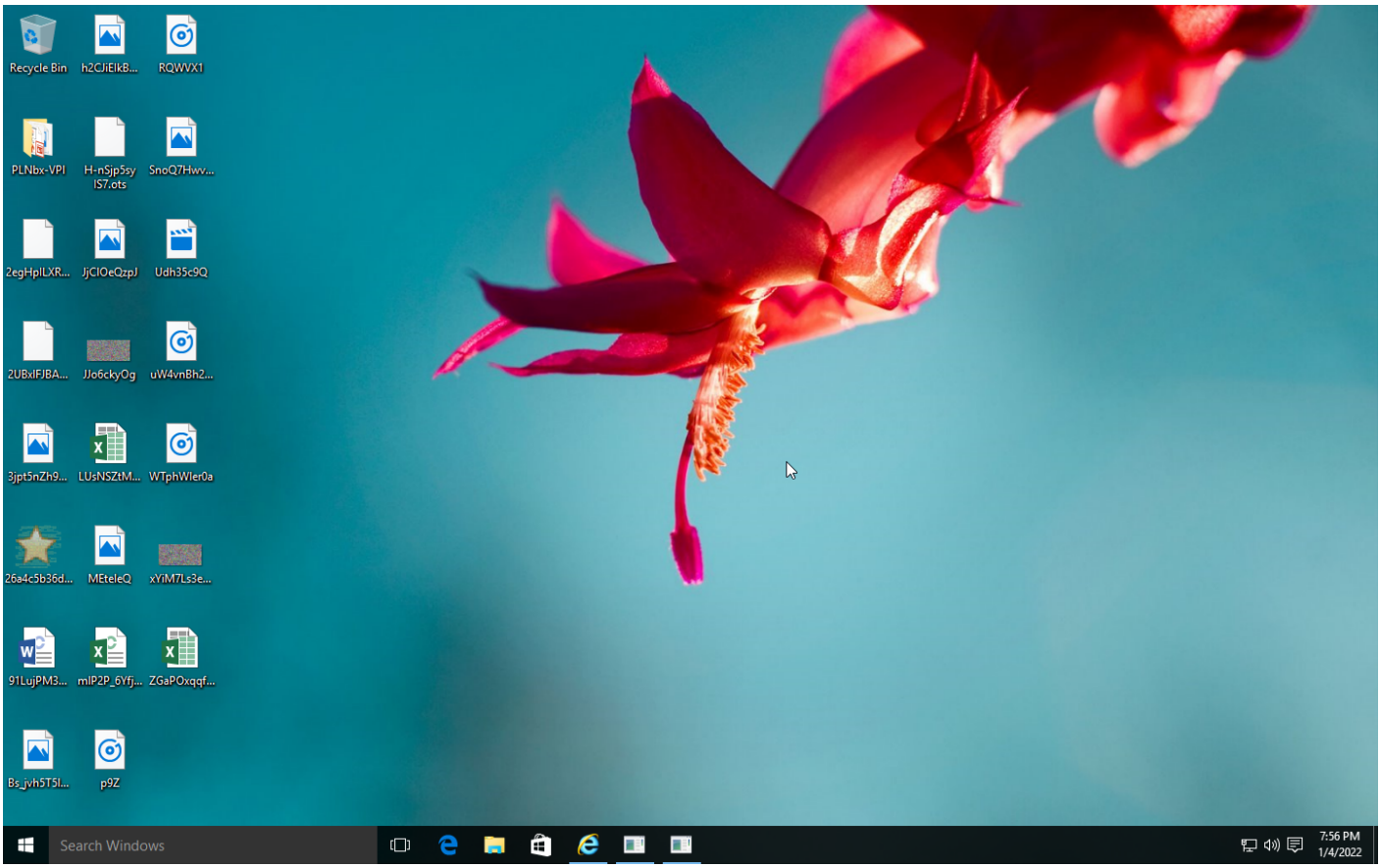
ID	#3231310
MD5	dc67c627917ff9724f3c1e6db5f2dc27
SHA1	4b7528999ad6095b3fbb3aec059efb88d999ea95
SHA256	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da
SSDeep	6144:5lA3X2bDueST6gKO1tqT7b4YlCTFGbGQ273pQGfT:5lA3X22e0VKYY70A4FOGQKt
ImpHash	e64508a754c560e6e71788b6f0d7d44d
File Name	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe
File Size	335.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

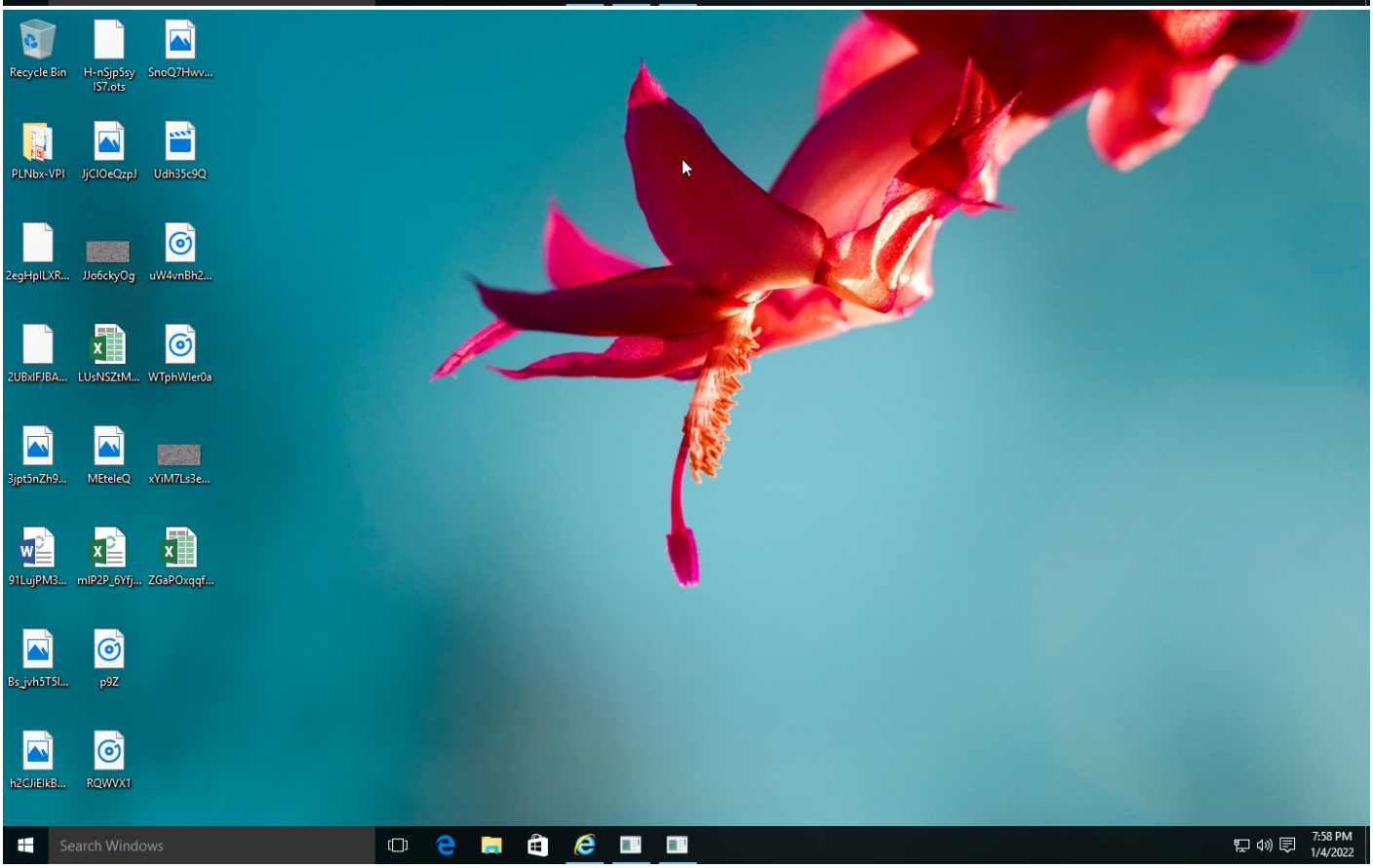
Analysis Information

Creation Time	2022-01-04 20:55 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
Execution Successful	False
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	3


Recycle Bin
h2CJiElkB...
RQWVX1
PLNbx-VPI
H-nSjp5sy
lS7.ots
SnoQ7Hwv...
2egHplLXR...
JjCIOeQzpJ
Udh35c9Q
2UBxlFJBA...
JJo6ckyOg
uW4vnBh2...
3jpt5nZh9...
LUsNSZtM...
WTphWIer0a
26a4c5b36d...
MEteleQ
xYiM7Ls3e...
91LujPM3...
mIP2P_6Yfj...
ZGaPOxqqf...
Bs_jvh5T5l...
p9Z
Search Windows
7:56 PM
1/4/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

15.62 KB total sent

1851.75 KB total received

2 ports 80, 20000

2 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

24 sessions, 15.62 KB sent, 1851.75 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	host-data-coin-11.com/	-	-		0 bytes	NA
GET	185.206.212.165/build_dl	-	-		0 bytes	NA

BEHAVIOR

Process Graph

Process #1: 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 67433, Reason: Analysis Target
Unmonitor End Time	End Time: 88081, Reason: Terminated
Monitor duration	20.65s
Return Code	0
PID	3260
Parent PID	1560
Bitness	32 Bit

Host Behavior

Type	Count
Module	71
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: 26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81939, Reason: Child Process
Unmonitor End Time	End Time: 99841, Reason: Terminated
Monitor duration	17.90s
Return Code	0
PID	1608
Parent PID	3260
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0x51c	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0x51c	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0x51c	0x367008(3567624)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0x51c / 0xed0	0x77c08fe0(2009108448)	-	✓	1

Host Behavior

Type	Count
Module	17
Keyboard	2
Process	1
File	1
System	6
-	1
Registry	12
-	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 95523, Reason: Injection
Unmonitor End Time	End Time: 309583, Reason: Terminated by Timeout
Monitor duration	214.06s
Return Code	Unknown
PID	1560
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0xed0	0x410000(4259840)	0x5000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0xed0	0x420000(4325376)	0x16000	✓	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	0xed0	0x421930(4331824)	-	✓	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	335.00 KB	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.exe	1791.00 KB	8c4294e3154675cd926ab6b772dbbe0e7a49cae16f4a37d908e1ca6748251c43	✗

Host Behavior

Type	Count
Module	61
System	46473
Process	6763
Mutex	1
Registry	2
File	55
User	1
COM	1

Network Behavior

Type	Count
HTTP	24
TCP	24

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: 131259, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 309583, Reason: Terminated by Timeout
Monitor duration	178.32s
Return Code	Unknown
PID	860
Parent PID	532
Bitness	64 Bit

Process #5: bcatcih

ID	5
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 142151, Reason: Child Process
Unmonitor End Time	End Time: 309583, Reason: Terminated by Timeout
Monitor duration	167.43s
Return Code	Unknown
PID	1944
Parent PID	860
Bitness	32 Bit

Host Behavior

Type	Count
Module	27
File	3
Environment	1

Process #6: 506a.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\506a.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 262651, Reason: Child Process
Unmonitor End Time	End Time: 309583, Reason: Terminated by Timeout
Monitor duration	46.93s
Return Code	Unknown
PID	2452
Parent PID	1560
Bitness	64 Bit

Host Behavior

Type	Count
Module	50
System	1
Environment	1
-	8

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da	C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	335.00 KB	application/vnd.microsoft.portable-executable	Delete, Create, Write, Access	MALICIOUS
8c4294e3154675cd926ab6b772dbbe0e7a49cae16f4a37d908e1ca6748251c43	C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.exe	Downloaded File	1791.00 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	SUSPICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	Sample File	Delete, Access	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	Delete, Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Delete, Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.tmp	Accessed File	Delete, Create, Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.exe	Downloaded File	Create, Write, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-data-coin-11.com	-	89.223.65.17	-	POST	MALICIOUS
http://185.206.212.165/build_dl	-	185.206.212.165	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
host-data-coin-11.com	89.223.65.17	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
89.223.65.17	host-data-coin-11.com	Russia	HTTP, TCP, DNS	CLEAN
185.206.212.165	-	Netherlands	HTTP, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
FE7F15060B875FB9FB2A49F08D5D03120C287F38	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE	access	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	read, access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe	"C:\Users\RDhJ0CNFevzX\Desktop\26a4c5b36d9fde80ea47137eb53b40dacf240432a5895f98417eae51b6b681da.exe"	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
506a.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\506A.exe	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	function_strings_process_3.txt	Downloader	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
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	Not installed

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