MALICIOUS

Classifications: Injector, Downloader

Threat Names: C2/Generic-A, SmokeLoader

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**0f5806e0887c0d85e43e46fa9aaecda2.exe**
ID	#9503289
MD5	0f5806e0887c0d85e43e46fa9aaecda2
SHA1	c6ba6e91d40aa1507775077f9662ecb25c9f0943
SHA256	dcd883af6eb91aa30a58838db875b23a981a14636c7c9cc3bcaba600ff8e034e
File Size	2327.00 KB
Report Created	2023-12-18 00:26 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 21 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Smoke Loader configuration was extracted	1	Downloader
	• A configuration for Smoke Loader was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Downloader
	• YARA detected "SmokeLoader" from ruleset "Malware" in memory dump data from (process #3) 5ih0dp8.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #3) 5ih0dp8.exe creates thread in (process #4) explorer.exe.			
4/5	Reputation	Malicious file detected via reputation	2	-
	• Embedded file "5IH0Dp8.exe" is a known malicious file. • The sample itself is a known malicious file.			
4/5	Reputation	Malicious host or URL detected via reputation	1	-
	• Reputation analysis labels the contacted IP address 144.76.136.153 as C2/Generic-A.			
3/5	YARA	Suspicious content matched by YARA rules	3	-
	• YARA detected "VMProcessNames" from ruleset "Generic" in function strings data from (process #3) 5ih0dp8.exe. • YARA detected "VMModuleNames" from ruleset "Generic" in function strings data from (process #3) 5ih0dp8.exe. • YARA detected "VMDeviceStrings" from ruleset "Generic" in function strings data from (process #3) 5ih0dp8.exe.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) 2dt5311.exe reads the network adapters' addresses by API.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #3) 5ih0dp8.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #1) 0f5806e0887c0d85e43e46fa9aaecda2.exe deletes executed executable "C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\5IH0Dp8.exe". • (Process #1) 0f5806e0887c0d85e43e46fa9aaecda2.exe deletes executed executable "C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\2dT5311.exe".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) 0f5806e0887c0d85e43e46fa9aaecda2.exe adds "rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\"" to Windows startup via registry.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 0f5806e0887c0d85e43e46fa9aaecda2.exe starts (process #2) 2dt5311.exe with a hidden window. • (Process #1) 0f5806e0887c0d85e43e46fa9aaecda2.exe starts (process #3) 5ih0dp8.exe with a hidden window.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #4) explorer.exe enumerates running processes.			
1/5	Network Connection	Performs DNS request	1	-

Score	Category	Operation	Count	Classification
	• (Process #2) 2dt5311.exe resolves hostname "transfer.sh" to IP "144.76.136.153".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) 2dt5311.exe opens an outgoing TCP connection to host "144.76.136.153:443".			
1/5	Execution	Executes dropped PE file	2	-
	• Executes dropped file "5IH0Dp8.exe". • Executes dropped file "2dT5311.exe".			

Malware Configuration: SmokeLoader

Metadata	Key	Extracted Value
Mission ID	Value	2022
Encryption Key	Key Tags Algorithm Key Tags Algorithm	7YOmbg== Network Communication Decryption Key RC4 tgl7Sw== Network Communication Encryption Key RC4
URL	Url	http://185.215.113.68/fks/index.php

Mitre ATT&CK Matrix

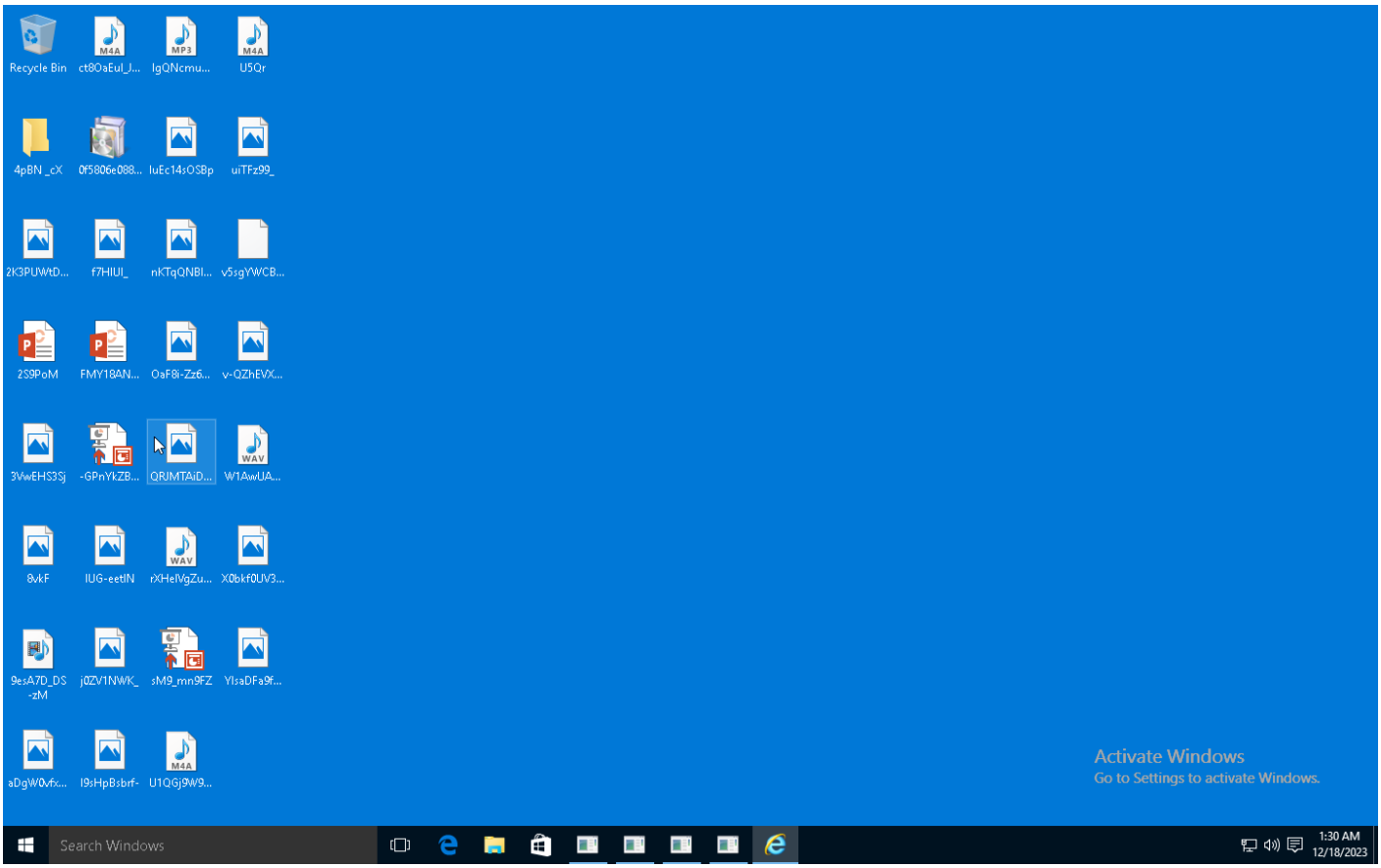
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry		#T1016 System Network Configuration Discovery					
				#T1143 Hidden Window		#T1057 Process Discovery					

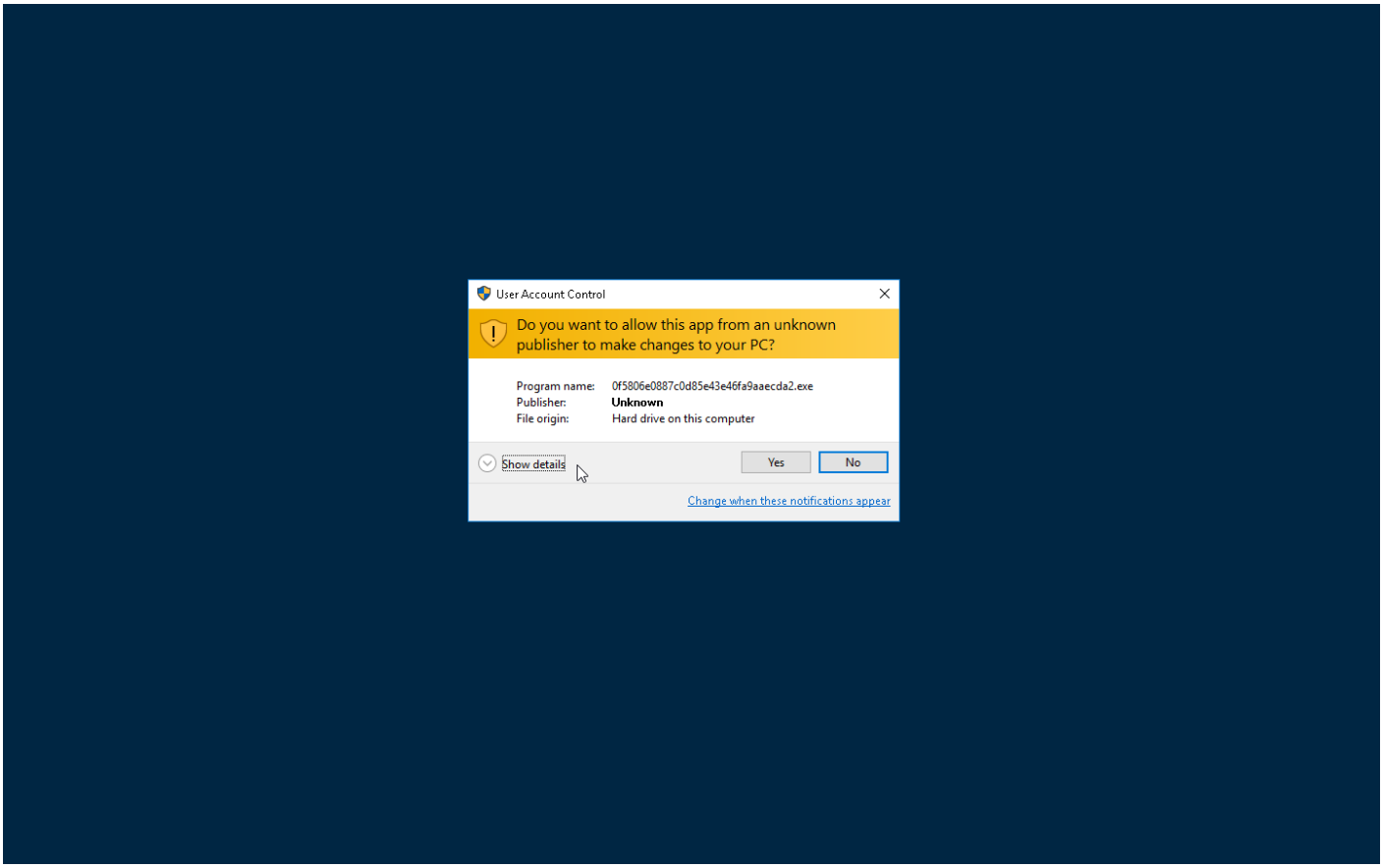
Sample Information

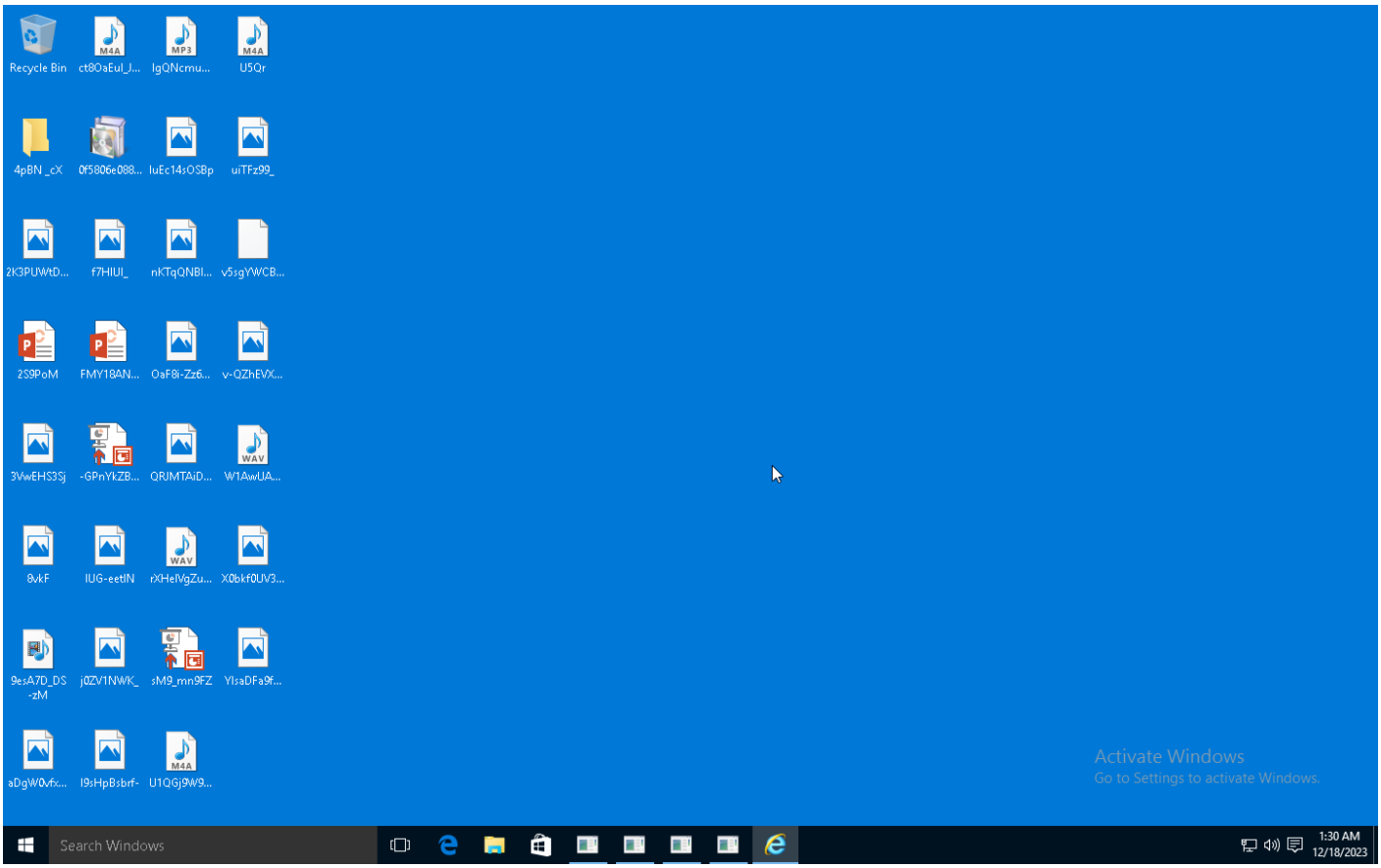
ID	#9503289
MD5	0f5806e0887c0d85e43e46fa9aaecda2
SHA1	c6ba6e91d40aa1507775077f9662ecb25c9f0943
SHA256	dcd883af6eb91aa30a58838db875b23a981a14636c7c9cc3bcaba600ff8e034e
SSDeep	49152:fUvSnJLx54y5aPWqnkOsbcpkQ1NOwMdwrHQ2mujs3wwpe0ORhxttB+:USnJLx54yl34bc2wEKnmUwpHORhdB+
ImpHash	646167cce332c1c252cdcb1839e0cf48
File Name	0f5806e0887c0d85e43e46fa9aaecda2.exe
File Size	2327.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-12-18 00:26 (UTC)
Analysis Duration	00:01:12
Termination Reason	Timeout
Number of Monitored Processes	4
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	5


Recycle Bin
Activate Windows
Go to Settings to activate Windows.
Search Windows
1:30 AM
12/18/2023


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 0f5806e0887c0d85e43e46fa9aaecda2.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
Activate Windows
Go to Settings to activate Windows.
Search Windows
1:30 AM
12/18/2023

NETWORK

General

209 bytes total sent

73 bytes total received

2 ports 443, 53

2 contacted IP addresses

1 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

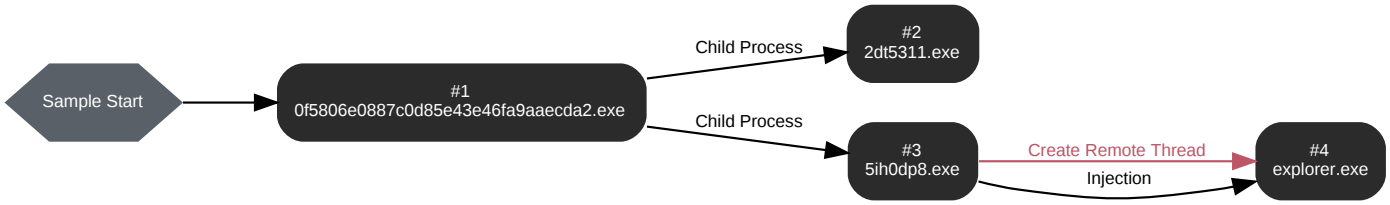
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	transfer[.]sh	NO_ERROR	144.76.136.153	-	CLEAN

BEHAVIOR

Process Graph



Process #1: 0f5806e0887c0d85e43e46fa9aaecda2.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\0f5806e0887c0d85e43e46fa9aaecda2.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\0f5806e0887c0d85e43e46fa9aaecda2.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 250157, Reason: Analysis Target
Unmonitor End Time	End Time: 310813, Reason: Terminated
Monitor duration	60.66s
Return Code	0
PID	4580
Parent PID	2024
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\5IH0Dp8.exe	36.61 KB	df09728a6383db0b8bb9f28a04ccd0c358e3f525c1d340c94d481fe8c97b4adb	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\TMP4351$.TMP	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\2dT5311.exe	3289.50 KB	e323b5052539a7aae8f60696811c3d6a80f6acc23071b3bbc032fa5f4616c3d3	✖

Host Behavior

Type	Count
Module	9
System	111
-	1
File	128
Process	8
Registry	11

Process #2: 2dt5311.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\ixp000.tmp\2dt5311.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\2dT5311.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\
Monitor Start Time	Start Time: 255833, Reason: Child Process
Unmonitor End Time	End Time: 301403, Reason: Terminated
Monitor duration	45.57s
Return Code	0
PID	1088
Parent PID	4580
Bitness	32 Bit

Host Behavior

Type	Count
Registry	27
Module	105
Window	16
System	11
File	19
-	1
-	10
Environment	4
-	1
Keyboard	3

Network Behavior

Type	Count
DNS	1
TCP	1

Process #3: 5ih0dp8.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\ixp000.tmp\5ih0dp8.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\5IH0Dp8.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\
Monitor Start Time	Start Time: 300413, Reason: Child Process
Unmonitor End Time	End Time: 309656, Reason: Terminated
Monitor duration	9.24s
Return Code	0
PID	5000
Parent PID	4580
Bitness	32 Bit

Host Behavior

Type	Count
Module	17
Keyboard	2
File	1
System	6
-	1
Registry	14

Process #4: explorer.exe

ID	4
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 306429, Reason: Injection
Unmonitor End Time	End Time: 321669, Reason: Terminated by timeout
Monitor duration	15.24s
Return Code	Unknown
PID	2024
Parent PID	-
Bitness	64 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Create Remote Thread	#3: c:\users\rdhj0cnfevzx\appdata\local\temp\ixp000.tmp\5ih0dp8.exe	0x1390	0x2370000(37158912)	-	✔	1

Host Behavior

Type	Count
Module	19
System	489
Process	530

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dcd883af6eb91aa30a58838db875b23a981a14636c7c9cc3bcaba600ff8e034e	C:\Users\RDhJ0CNFevzX\Desktop\0f5806e0887c0d85e43e46fa9aaecda2.exe	Sample File	2327.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
e4650d5c5529391f0648eb3e4c4db6342d6eff957ef49dcb1e17f6e3d3f42cde	-	Extracted File	2183.97 KB	application/vnd.ms-cab-compressed	-	MALICIOUS
df09728a6383db0b8bb9f28a04ccd0c358e3f525c1d340c94d481fe8c97b4adb	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\5IH0Dp8.exe, 5IH0Dp8.exe	Archive File	36.61 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
4cad27c3790c5375ffa8066c783e2664f42effe54280ce5a381b3e641765f219	-	Memory Dump	24.00 KB	application/x-dbt	-	MALICIOUS
5350f565ba1c09043407069b7ee107b71083707574e868021cfbcad79b1e7a86	-	Memory Dump	88.00 KB	application/octet-stream	-	MALICIOUS
e323b5052539a7aae8f60696811c3d6a80f6acc23071b3bbc032fa5f4616c3d3	2dT5311.exe, C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\2dT5311.exe	Archive File	3289.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	SUSPICIOUS
f169eed8248d8f9efd20dd716790f2b3bb0547687546811b4137be21b5c63b71	-	Extracted File	54.46 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\0f5806e0887c0d85e43e46fa9aaecda2.exe	Accessed File, Sample File	Access	MALICIOUS
2dT5311.exe	Miscellaneous File	-	CLEAN
5IH0Dp8.exe	Miscellaneous File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\TMP4351$.TMP	Accessed File, Dropped File	Access, Create, Delete	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\2dT5311.exe	Accessed File, Dropped File, Extracted File	Access, Create, Delete, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\5IH0Dp8.exe	Accessed File, Dropped File, Extracted File	Access, Create, Delete, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP	Accessed File	Access, Create, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\IXP000.TMP\2dT5311.exe.config	Accessed File	Access	CLEAN
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\system32\ntdll.dll	Accessed File	Access	CLEAN
rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\	Miscellaneous File	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://185[.]215[.]113[.]68/fks/index.php	Extracted	185.215.113.68	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
transfer[.]sh	144.76.136.153	Germany	TCP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
144.76.136.153	transfer[.]sh	Germany	TCP, DNS	MALICIOUS
185.215.113.68	-	-	-	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager	access	0f5806e0887c0d85e43e46fa9aaecda2.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations	access, read	0f5806e0887c0d85e43e46fa9aaecda2.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce	access, create	0f5806e0887c0d85e43e46fa9aaecda2.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup0	access, write, delete, read	0f5806e0887c0d85e43e46fa9aaecda2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	2dt5311.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	2dt5311.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	2dt5311.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	2dt5311.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	2dt5311.exe	CLEAN

Process

Process Name	Commandline	Verdict
5ih0dp8.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\5IH0Dp8.exe	MALICIOUS
0f5806e0887c0d85e43e46fa9aaecda2.exe	"C:\Users\RDhJ0CNFevzX\Desktop\0f5806e0887c0d85e43e46fa9aaecda2.exe"	MALICIOUS
2dt5311.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\IXP000.TMP\2dT5311.exe	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS

YARA / AV

YARA (5)

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
Generic	VMProcessNames	VM detection via known process names	Function Strings	-	-	3/5
Generic	VMModuleNames	VM detection via known module names	Function Strings	-	-	3/5
Generic	VMDeviceStrings	VM detection via known device names	Function Strings	-	-	3/5

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	2023.4.1
Dynamic Engine Version	2023.4.1 / 11/10/2023 05:23
Static Engine Version	2023.4.1.0 / 2023-11-10 04:00:12
AV Exceptions Version	2023.4.1.4 / 2023-09-25 17:49:30
Link Detonation Heuristics Version	2023.4.1.48 / 2023-11-30 16:07:35
Smart Memory Dumping Rules Version	2023.4.1.4 / 2023-09-25 17:49:30
Config Extractors Version	2023.4.1.48 / 2023-11-30 16:07:35
Signature Trust Store Version	2023.4.1.4 / 2023-09-25 17:49:30
VMRay Threat Identifiers Version	2023.4.1.56 / 2023-12-06 21:36:31
YARA Built-in Ruleset Version	2023.4.1.48

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