MALICIOUS

Classifications: Spyware

Threat Names: FormBook

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe**
ID	#3401039
MD5	5e9af5b2056e4da639a9459e3b36193c
SHA1	b779402e9a6ecbbef6b68817814991bbcade12df
SHA256	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d
File Size	523.00 KB
Report Created	2022-01-31 12:08 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 16 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "FormBook_2021" from ruleset "Malware" has matched on a memory dump for (process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe.			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe modifies memory of (process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe alters context of (process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe.			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\KHDScDG.exe", to be triggered by Logon.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	4	-
	• (Process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe makes a direct system call to "NtQuerySystemInformation". • (Process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe makes a direct system call to "NtQueryInformationProcess". • (Process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe makes a direct system call to "NtAllocateVirtualMemory". • (Process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe makes a direct system call to "NtFreeVirtualMemory".			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe starts (process #3) schtasks.exe with a hidden window. • (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe starts (process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe reads from (process #7) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Execution	Executes itself	1	-
	• (Process #1) 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe.			

Mitre ATT&CK Matrix

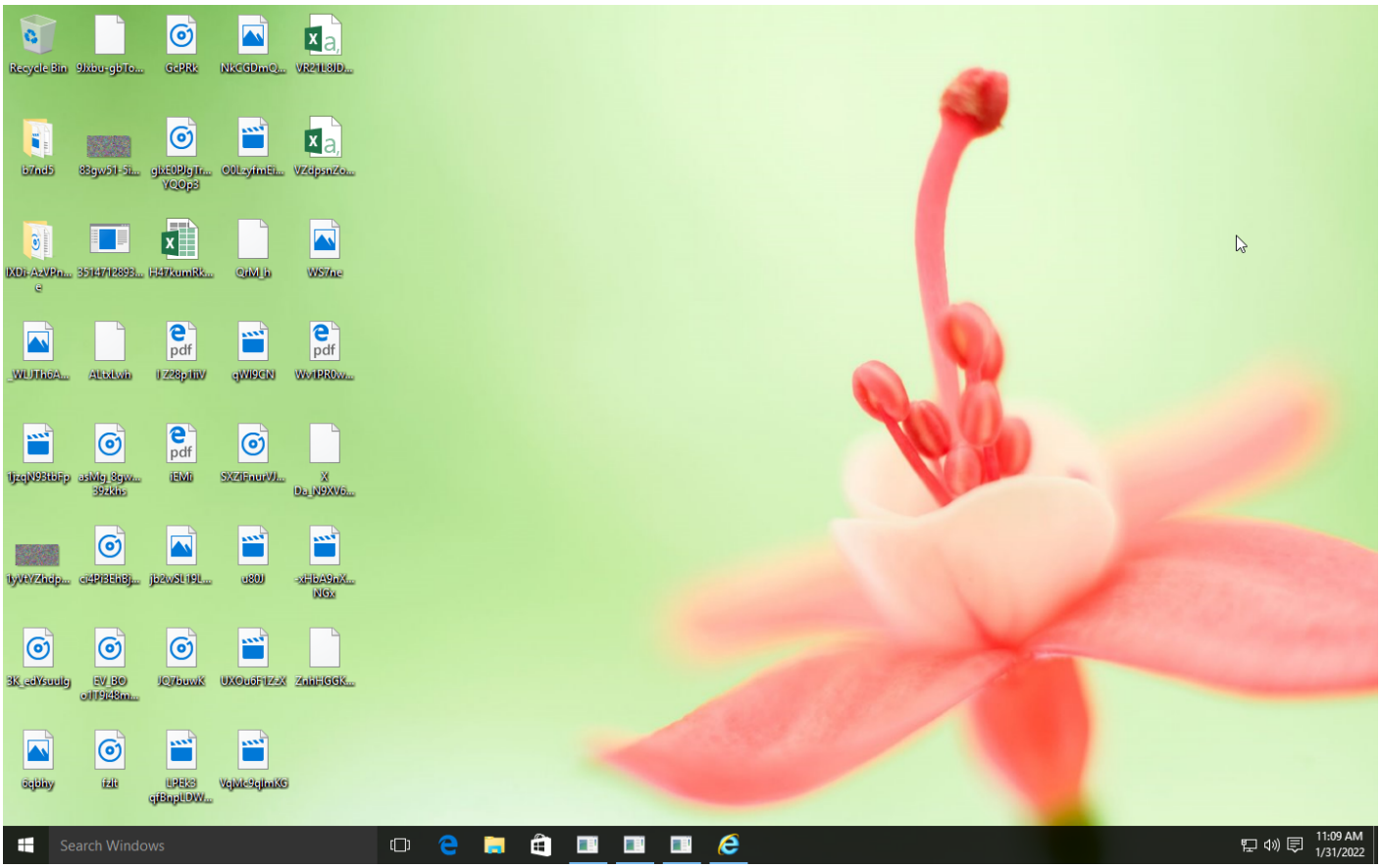
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window							
				#T1045 Software Packing							

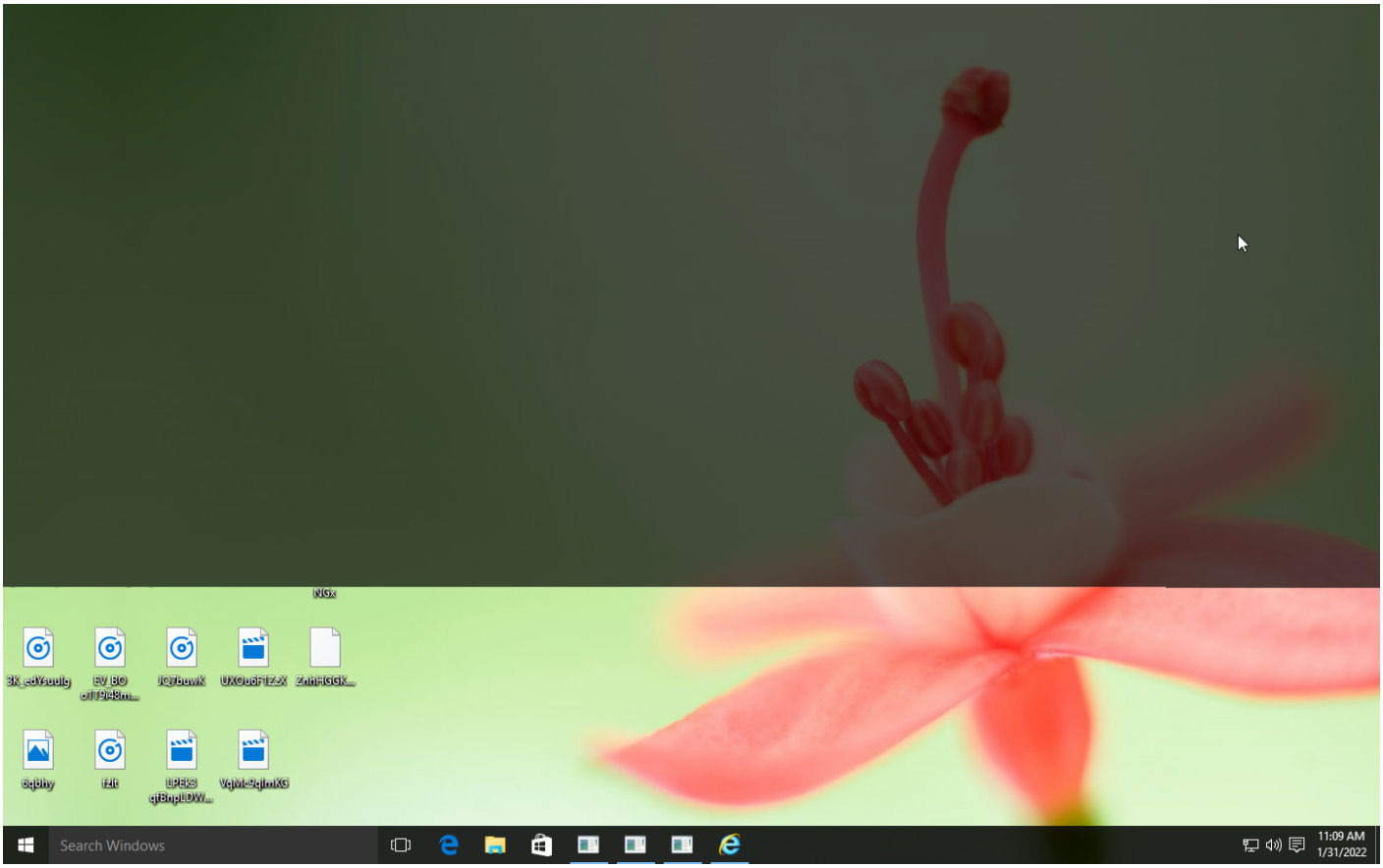
Sample Information

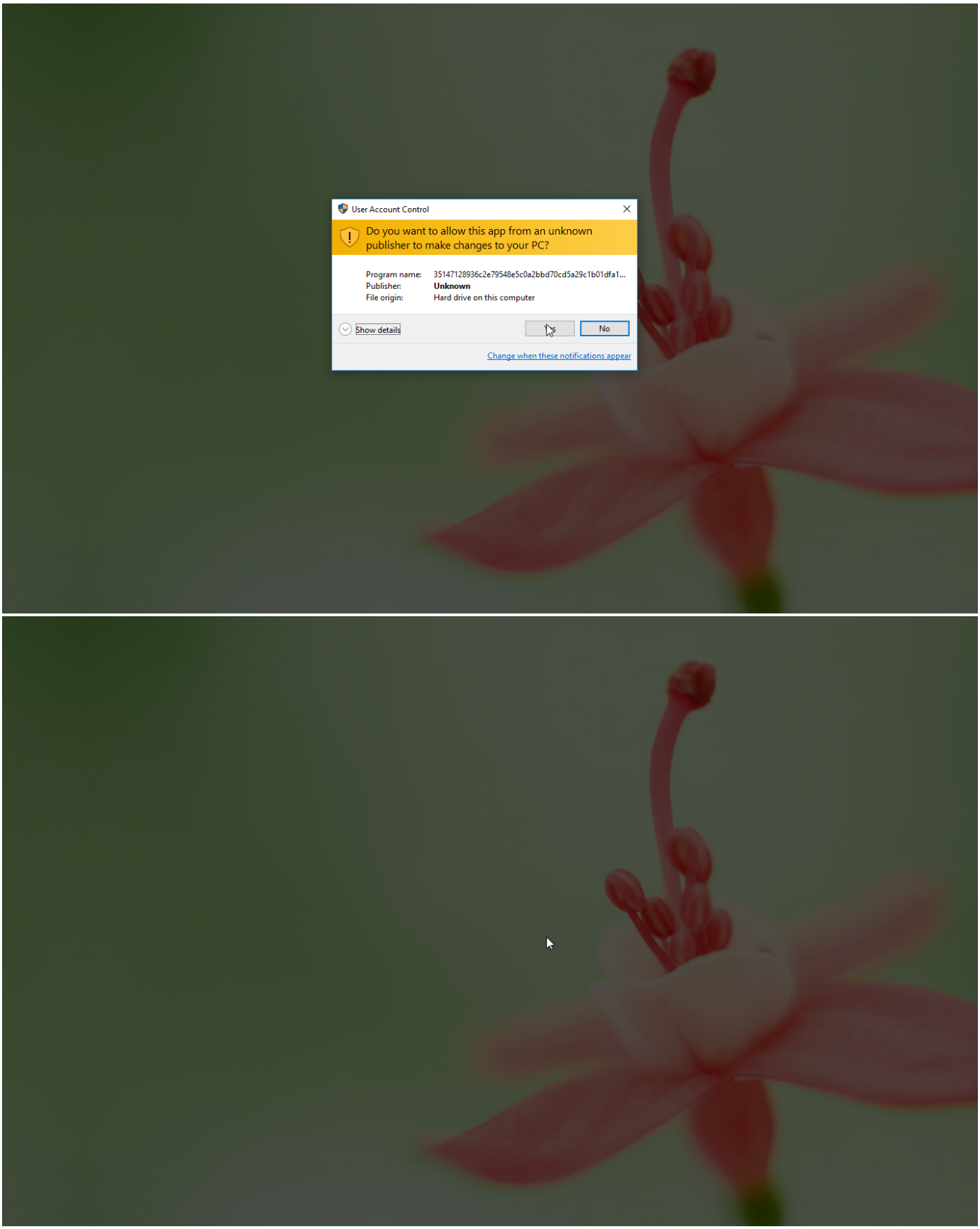
ID	#3401039
MD5	5e9af5b2056e4da639a9459e3b36193c
SHA1	b779402e9a6ecbbef6b68817814991bbcade12df
SHA256	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d
SSDeep	12288:KcqT+JVO7JUQ1h1038w3pym2sdklRwCk3:KcqcVOV3h103s0waH
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe
File Size	523.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-01-31 12:08 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
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	1


Recycle Bin
Search Windows
11:09 AM
1/31/2022


Search Windows
11:09 AM
1/31/2022



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

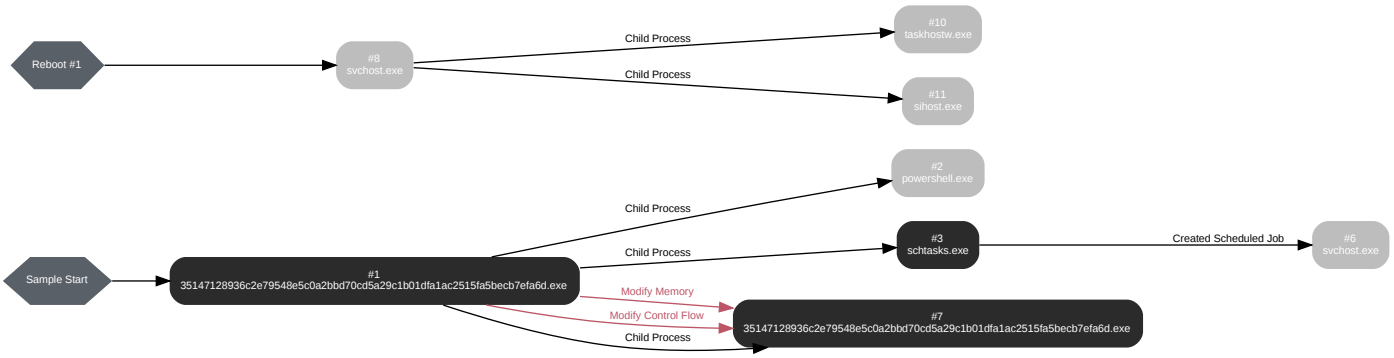
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 80131, Reason: Analysis Target
Unmonitor End Time	End Time: 209713, Reason: Terminated
Monitor duration	129.58s
Return Code	0
PID	4052
Parent PID	1560
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\KHDScDG.exe	523.00 KB	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC2CF.tmp	1.56 KB	88c520f6470da06d6682104a1d1b9cc26ebbb34b42b04dddc194d7c018d81e3d	✗

Host Behavior

Type	Count
Module	79
Window	6
Registry	3
Process	3
File	58
User	1
-	3
-	5

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\KHDScDG.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 181697, Reason: Child Process
Unmonitor End Time	End Time: 230808, Reason: Terminated
Monitor duration	49.11s
Return Code	1073807364
PID	3696
Parent PID	4052
Bitness	32 Bit

Process #3: schtasks.exe

ID	3
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KHDScDG" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC2CF.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 182272, Reason: Child Process
Unmonitor End Time	End Time: 207190, Reason: Terminated
Monitor duration	24.92s
Return Code	0
PID	3836
Parent PID	4052
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	10

Process #6: svchost.exe

ID	6
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: 203648, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 320221, Reason: Terminated by Timeout
Monitor duration	116.57s
Return Code	Unknown
PID	860
Parent PID	532
Bitness	64 Bit

Process #7: 35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206677, Reason: Child Process
Unmonitor End Time	End Time: 210552, Reason: Terminated
Monitor duration	3.88s
Return Code	0
PID	3128
Parent PID	4052
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\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	0xda0	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	0xda0	0x401000(4198400)	0x2d400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	0xda0	0x2db008(2994184)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	0xda0 / 0x448		-	✓	1

Host Behavior

Type	Count
File	5
-	1
-	1
System	2

Process #8: svchost.exe

ID	8
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: 264940, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 320221, Reason: Terminated by Timeout
Monitor duration	55.28s
Return Code	Unknown
PID	1004
Parent PID	536
Bitness	64 Bit

Process #10: taskhostw.exe

ID	10
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe TpmTasks
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 299869, Reason: Child Process
Unmonitor End Time	End Time: 320221, Reason: Terminated by Timeout
Monitor duration	20.35s
Return Code	Unknown
PID	1348
Parent PID	1004
Bitness	64 Bit

Process #11: sihost.exe

ID	11
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 315269, Reason: Child Process
Unmonitor End Time	End Time: 320221, Reason: Terminated by Timeout
Monitor duration	4.95s
Return Code	Unknown
PID	1564
Parent PID	1004
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d	C:\Users\RDhJ0CNFevzX\AppData\Roaming\KHDScDG.exe, C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	Sample File	523.00 KB	application/vnd.microsoft.portable-executable	Create, Write, Access	MALICIOUS
88c520f6470da06d6682104a1d1b9cc26ebbb34b42b04ddddc194d7c018d81e3d	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC2CF.tmp	Dropped File	1.56 KB	text/xml	Read, Delete, Create, Write, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Honda\35147128936c2e79548e5c0a2_Url_42zafj2lpxfbh2ahd0lrlhbdwhiagxdp\12.1.9.0\user.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Honda\35147128936c2e79548e5c0a2_Url_42zafj2lpxfbh2ahd0lrlhbdwhiagxdp\12.1.9.0\user.config	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\KHDScDG.exe	Sample File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC2CF.tmp	Dropped File	Read, Delete, Create, Write, Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
\??\C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Create, Read, Access	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	CLEAN

Process

Process Name	Commandline	Verdict
35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	"C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe"	MALICIOUS
35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe	"C:\Users\RDhJ0CNFevzX\Desktop\35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d.exe"	SUSPICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KHDScDG" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC2CF.tmp"	SUSPICIOUS

Process Name	Commandline	Verdict
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\KHDScDG.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskhostw.exe	taskhostw.exe TpmTasks	CLEAN
sihost.exe	sihost.exe	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	FormBook_2021	FormBook	Memory Dump	-	Spyware	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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
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	4.4.1.0 / 2022-01-14 04:00:58
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	4.4.1.9

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