MALICIOUS

Classifications: Injector | Downloader

Threat Names: SmokeLoader | Mal/Generic-S | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe**
ID	#5056619
MD5	c9948059cdc5e0aef9c193d605c7f659
SHA1	0c00b2242c86487e305d53aea8894100bda41035
SHA256	80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b
File Size	182.00 KB
Report Created	2022-08-03 22:21 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (25 rules, 37 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	3	Downloader
	• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.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) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe creates thread in (process #3) explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "http://host-file-host6.com/" which was contacted by (process #3) explorer.exe as Mal/HTMLGen-A.			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "host-file-host6.com" as Mal/HTMLGen-A.			
3/5	YARA	Suspicious content matched by YARA rules	3	-
	• Rule "VMDeviceStrings" from ruleset "Generic" has matched on the function strings for (process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe. • Rule "VMModuleNames" from ruleset "Generic" has matched on the function strings for (process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe. • Rule "VMProcessNames" from ruleset "Generic" has matched on the function strings for (process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.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\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.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 virtual machine	1	-

Score	Category	Operation	Count	Classification
	• (Process #9) 311b.exe is possibly trying to detect a VM via rdtsc.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	2	-
	• (Process #1) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe modifies memory of (process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe. • (Process #6) bcatcih modifies memory of (process #10) bcatcih.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	2	-
	• (Process #1) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe alters context of (process #2) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe. • (Process #6) bcatcih alters context of (process #10) bcatcih.			
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	2	-
	• (Process #1) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe reads from (process #1) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe. • (Process #6) bcatcih reads from (process #6) bcatcih.			
1/5	Obfuscation	Creates a page with write and execute permissions	2	-
	• (Process #1) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #6) bcatcih 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	Hide Tracks	Creates process with hidden window	2	-
	• (Process #3) explorer.exe starts (process #3) explorer.exe with a hidden window. • (Process #6) bcatcih starts (process #6) bcatcih with a hidden window.			
1/5	Network Connection	Downloads file	1	-
	• (Process #3) explorer.exe downloads file via http from http://host-file-host6.com.			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe resolves 39 API functions by name. • (Process #6) bcatcih resolves 39 API functions by name.			
1/5	Execution	Drops PE file	1	-
	• (Process #3) explorer.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe".			

Malware Configuration: SmokeLoader

Metadata	Key	Extracted Value
Mission ID	Value	2020
Encryption Key	Key Tags Algorithm	u4gEqg== Network Communication Decryption Key RC4
	Key Tags Algorithm	0vD4Mw== Network Communication Encryption Key RC4
URL	Url	http://host-file-host6.com/
	Url	http://host-host-file8.com/

Mitre ATT&CK Matrix

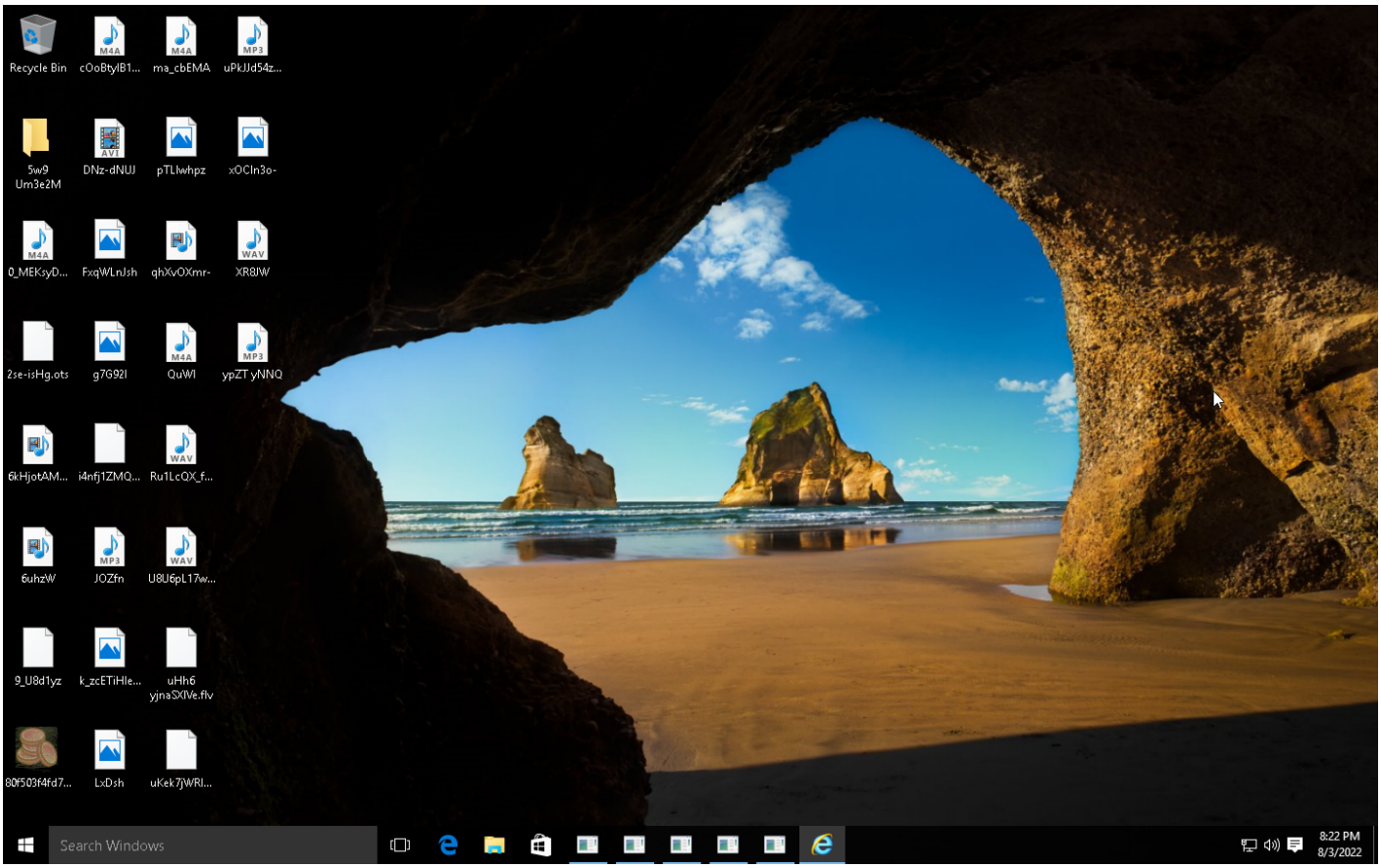
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
				#T1096 NTFS File Attributes		#T1497 Virtualization/ Sandbox Evasion			#T1105 Remote File Copy		
				#T1143 Hidden Window		#T1124 System Time Discovery					
				#T1497 Virtualization/ Sandbox Evasion							

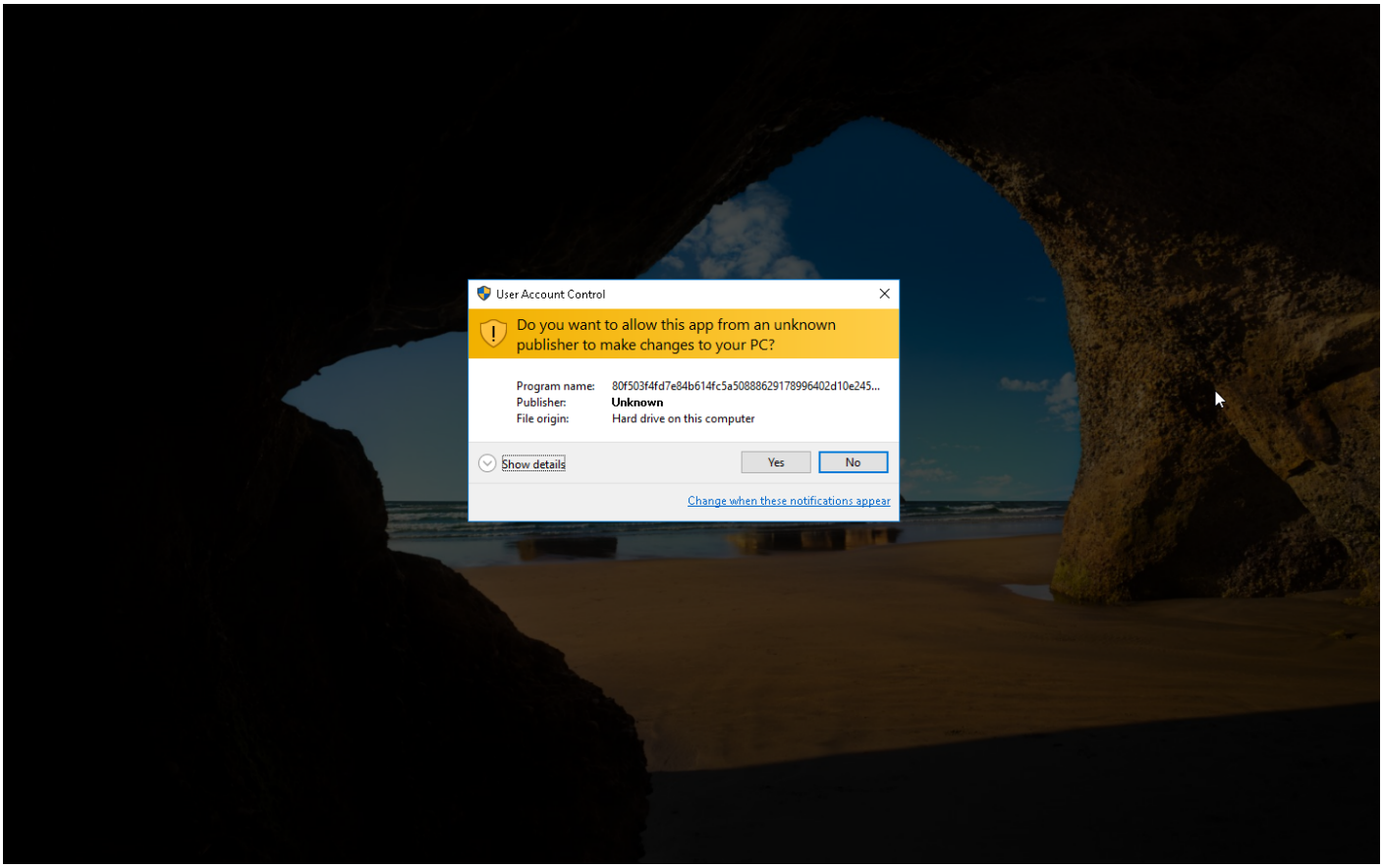
Sample Information

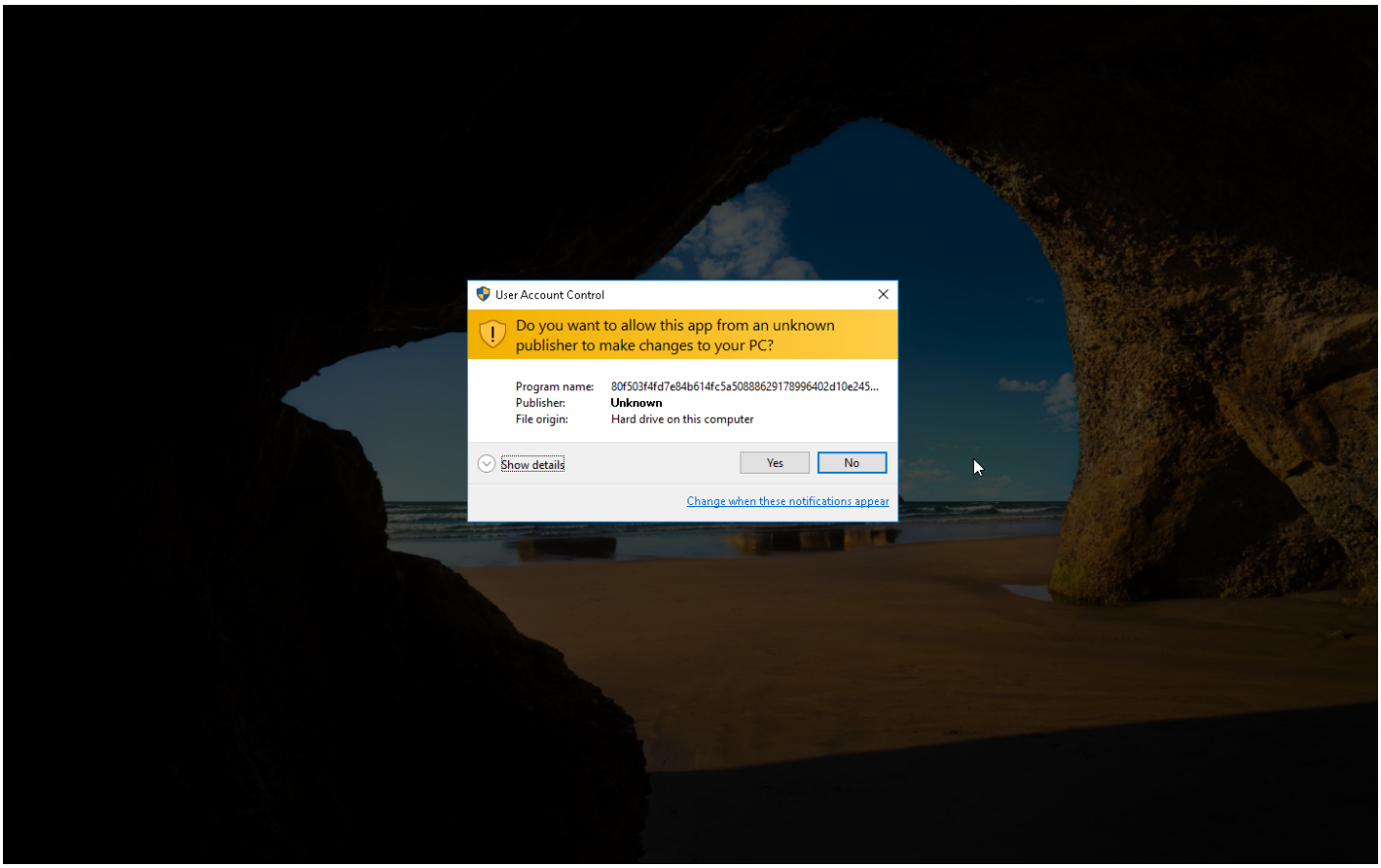
ID	#5056619
MD5	c9948059cdc5e0aef9c193d605c7f659
SHA1	0c00b2242c86487e305d53aea8894100bda41035
SHA256	80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b
SSDeep	3072:O1CItAzXunlpY2Tw4gST76X9JfIruFeKQvd4xlYCjwm3Y:OgSlIDwNS/6X9OihQvqb8m
ImpHash	19d26450af6fae284e6a28f691d90382
File Name	80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe
File Size	182.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-03 22:21 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	7
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	6


Recycle Bin
cOoBtylB1...
ma_cbEMA
uPkJJd54z...
5w9 Um3e2M
DNz-dNUJ
pTLlwhpz
xOCln3o-
0_MEKsyD...
FxqWLnJsh
qhXvOXmr-
XR8JW
2se-isHg.ots
g7G92I
QuWI
ypZTyNNQ
6kHjotAM...
i4nfj1ZMQ...
Ru1LcQX_f...
6uhzW
JOZfn
U8U6pL17w...
9_U8d1yz
k_zcETiHle...
uHh6 yjnaSXfVe.flv
80f503f4fd7...
LxDsh
uKek7jWRl...
Search Windows
8:22 PM
8/3/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 80f503f4fd7e84b614fc5a5088862917899640 2d10e245...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

23.03 KB total sent

4724.60 KB total received

3 ports 80, 443, 53

3 contacted IP addresses

1 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

3 sessions, 24.17 KB sent, 4725.13 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://host-file-host6.com	-	-		0 bytes	NA
GET	https://dl.uploadgram.me/62eab5c3587fah?raw	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	host-file-host6.com	NO_ERROR	34.118.39.10		NA
A	dl.uploadgram.me	NO_ERROR	176.9.247.226		NA

BEHAVIOR

Process Graph

Process #1: 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 60675, Reason: Analysis Target
Unmonitor End Time	End Time: 88406, Reason: Terminated
Monitor duration	27.73s
Return Code	0
PID	1552
Parent PID	1972
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	182.00 KB	80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b	✖

Host Behavior

Type	Count
Module	52
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: 80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81963, Reason: Child Process
Unmonitor End Time	End Time: 104080, Reason: Terminated
Monitor duration	22.12s
Return Code	0
PID	3064
Parent PID	1552
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\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0xad4	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0xad4	0x401000(4198400)	0x7200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0xad4	0x35d008(3526664)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0xad4 / 0x254	0x77248fe0(1998884832)	-	✔	1

Host Behavior

Type	Count
Module	17
Keyboard	2
File	1
System	6
-	1
Registry	14
Process	1
-	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: 97541, Reason: Injection
Unmonitor End Time	End Time: 305087, Reason: Terminated by timeout
Monitor duration	207.55s
Return Code	Unknown
PID	1972
Parent PID	-
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\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0x254	0x610000(6356992)	0x5000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0x254	0x1e80000(31981568)	0x16000	✔	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	0x254	0x1e81930(31988016)	-	✔	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	182.00 KB	80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe	4580.71 KB	2193ac16d10f2a4c968fde0ae2d654258c073d731641b7c13cb688f5fea2c515	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	21
System	4967
Process	16672
Mutex	1
Registry	2
File	15
User	1
COM	1

Network Behavior

Type	Count
HTTP	3
HTTPS	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: 135473, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 305087, Reason: Terminated by timeout
Monitor duration	169.61s
Return Code	Unknown
PID	864
Parent PID	1972
Bitness	64 Bit

Process #6: bcatcih

ID	6
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: 146842, Reason: Child Process
Unmonitor End Time	End Time: 302365, Reason: Terminated
Monitor duration	155.52s
Return Code	0
PID	3248
Parent PID	864
Bitness	32 Bit

Host Behavior

Type	Count
Module	52
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #9: 311b.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\311b.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 195781, Reason: Child Process
Unmonitor End Time	End Time: 305087, Reason: Terminated by timeout
Monitor duration	109.31s
Return Code	Unknown
PID	2956
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
System	8
Module	11
File	3
Environment	1

Process #10: bcatcih

ID	10
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: 271592, Reason: Child Process
Unmonitor End Time	End Time: 305087, Reason: Terminated by timeout
Monitor duration	33.49s
Return Code	Unknown
PID	4380
Parent PID	3248
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc8	0x400000(4194304)	0x200	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc8	0x401000(4198400)	0x7200	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc8	0x2f4008(3096584)	0x4	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih	0xcc8 / 0x678	0x77248fe0(1998884832)	-	✔	1

Host Behavior

Type	Count
Module	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih, C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	Sample File	182.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
a1aaaf3a627c8a4f9e25bd0ecb3b446a79fe46d1695d03790c8c8f89eba402dc	-	Downloaded File	407 bytes	text/html	-	CLEAN
9f37ee32b5f1620f44adc2a458c60e504a650419f2de2882c912792c3e0d8a93	-	Downloaded File	24 bytes	application/octet-stream	-	CLEAN
0b2cf6f19062846abe69598be7353f148c28d58882ace4487dd7e9e8e01a6449	-	Downloaded File	55 bytes	application/octet-stream	-	CLEAN
2193ac16d10f2a4c968fde0ae2d654258c073d731641b7c13cb688f5fea2c515	C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe	Dropped File	4580.71 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a50888629178996402d10e245193136c0aee909b87b.exe	Sample File, Accessed File, VM File	Access, Delete	MALICIOUS
C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa	Accessed File	Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
apfHQ	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-host-file8.com	-	-	-	-	MALICIOUS
http://host-file-host6.com	-	34.118.39.10	-	POST	MALICIOUS
https://dl.uploadgram.me/62eab5c3587fah?raw	-	176.9.247.226	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
host-file-host6.com	34.118.39.10	-	TCP, DNS, HTTP	MALICIOUS
host-host-file8.com	-	-	-	CLEAN
dl.uploadgram.me	176.9.247.226	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
176.9.247.226	dl.uploadgram.me	Germany	TCP, HTTPS, DNS	CLEAN
34.118.39.10	host-file-host6.com	Poland	TCP, DNS, HTTP	CLEAN

Mutex

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

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
80f503f4fd7e84b614fc5a5088862917899640 2d10e245193136c0aee909b87b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a5088862917899640 2d10e245193136c0aee909b87b.exe"	MALICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
80f503f4fd7e84b614fc5a5088862917899640 2d10e245193136c0aee909b87b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\80f503f4fd7e84b614fc5a5088862917899640 2d10e245193136c0aee909b87b.exe"	SUSPICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
311b.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\311B.exe	CLEAN

YARA / AV

YARA (6)

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

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.0.1 / 2022-07-04 05:54:12
Link Detonation Heuristics Version	4.6.0.3 / 2022-07-11 12:34:44
Smart Memory Dumping Rules Version	4.6.0.1 / 2022-07-04 05:54:12
Config Extractors Version	4.6.0.6 / 2022-07-25 08:17:36
Signature Trust Store Version	4.6.0.1 / 2022-07-04 05:54:12
VMRay Threat Identifiers Version	4.6.0.8 / 2022-07-26 09:34:25
YARA Built-in Ruleset Version	4.6.0.5

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	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