MALICIOUS

Classifications: Injector | Downloader

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**31646747fe74d32212a7cbcb97c7d78d.virus.exe**
ID	#3193620
MD5	31646747fe74d32212a7cbcb97c7d78d
SHA1	62df758f397934053749ee38416a74f81a6d8ed6
SHA256	02bcb080116ab55475edbcd1293246a0e5d8894793ee9e699db805bff2935408
File Size	331.50 KB
Report Created	2021-12-27 22:59 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (22 rules, 28 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) 31646747fe74d32212a7cbcb97c7d78d.virus.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) 31646747fe74d32212a7cbcb97c7d78d.virus.exe modifies memory of (process #3) explorer.exe.		
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) 31646747fe74d32212a7cbcb97c7d78d.virus.exe creates thread in (process #3) explorer.exe.		
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels file "C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.exe" as "Mal/Generic-S".		
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) 31646747fe74d32212a7cbcb97c7d78d.virus.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\31646747fe74d32212a7cbcb97c7d78d.virus.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) 8b87.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) 31646747fe74d32212a7cbcb97c7d78d.virus.exe modifies memory of (process #2) 31646747fe74d32212a7cbcb97c7d78d.virus.exe.		
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 31646747fe74d32212a7cbcb97c7d78d.virus.exe alters context of (process #2) 31646747fe74d32212a7cbcb97c7d78d.virus.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.		

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 31646747fe74d32212a7cbcb97c7d78d.virus.exe reads from (process #2) 31646747fe74d32212a7cbcb97c7d78d.virus.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 31646747fe74d32212a7cbcb97c7d78d.virus.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	Hide Tracks	Creates process with hidden window	1	-
	• (Process #3) explorer.exe starts (process #6) 8b87.exe with a hidden window.			
1/5	Execution	Executes itself	2	-
	• (Process #1) 31646747fe74d32212a7cbcb97c7d78d.virus.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe. • (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe.			
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	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) 31646747fe74d32212a7cbcb97c7d78d.virus.exe resolves 39 API functions by name. • (Process #6) 8b87.exe resolves 59 API functions by name.			

Mitre ATT&CK Matrix

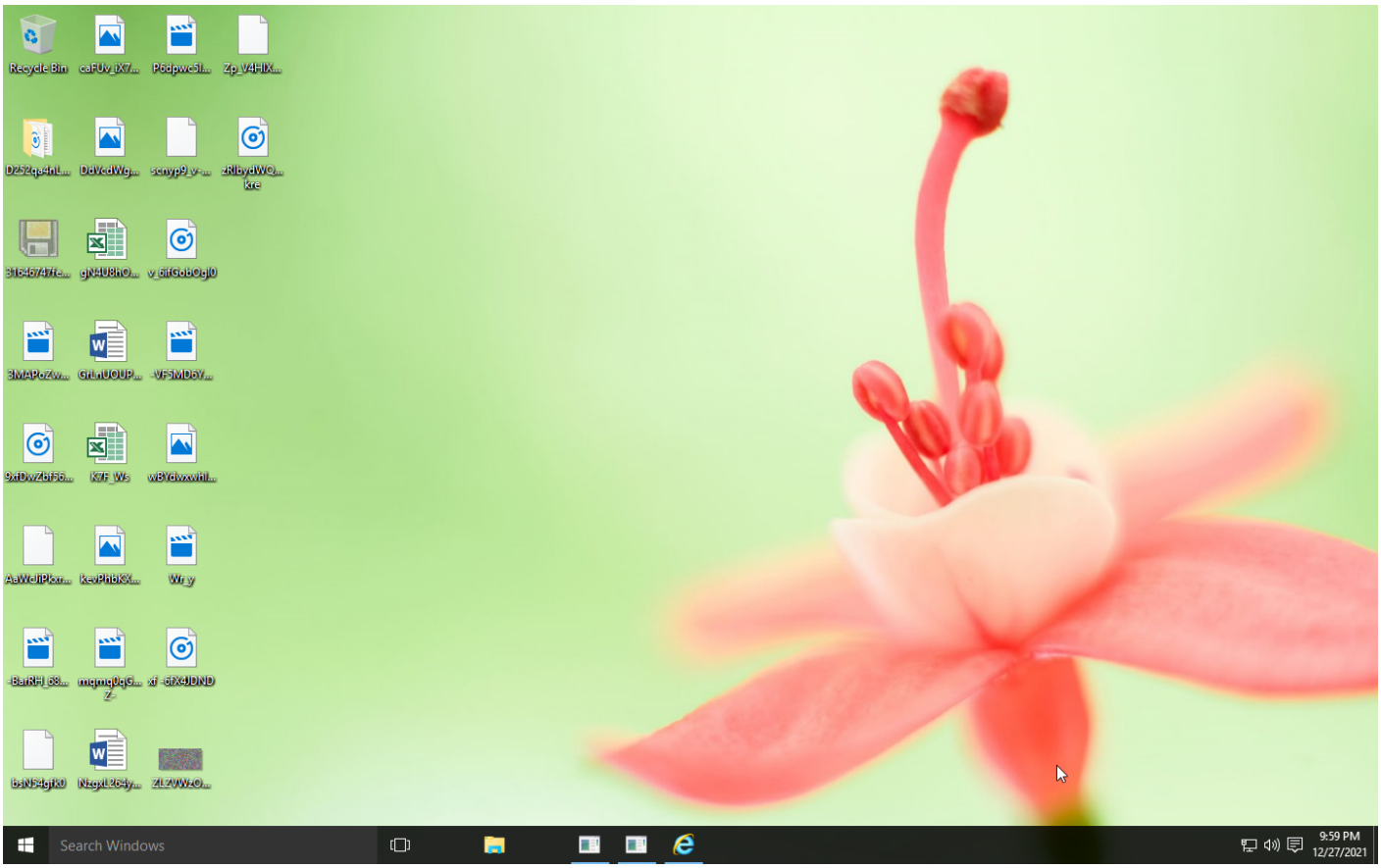
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
				#T1096 NTFS File Attributes		#T1497 Virtualization/ Sandbox Evasion			#T1105 Remote File Copy		
				#T1143 Hidden Window					#T1065 Uncommonly Used Port		
				#T1497 Virtualization/ Sandbox Evasion							

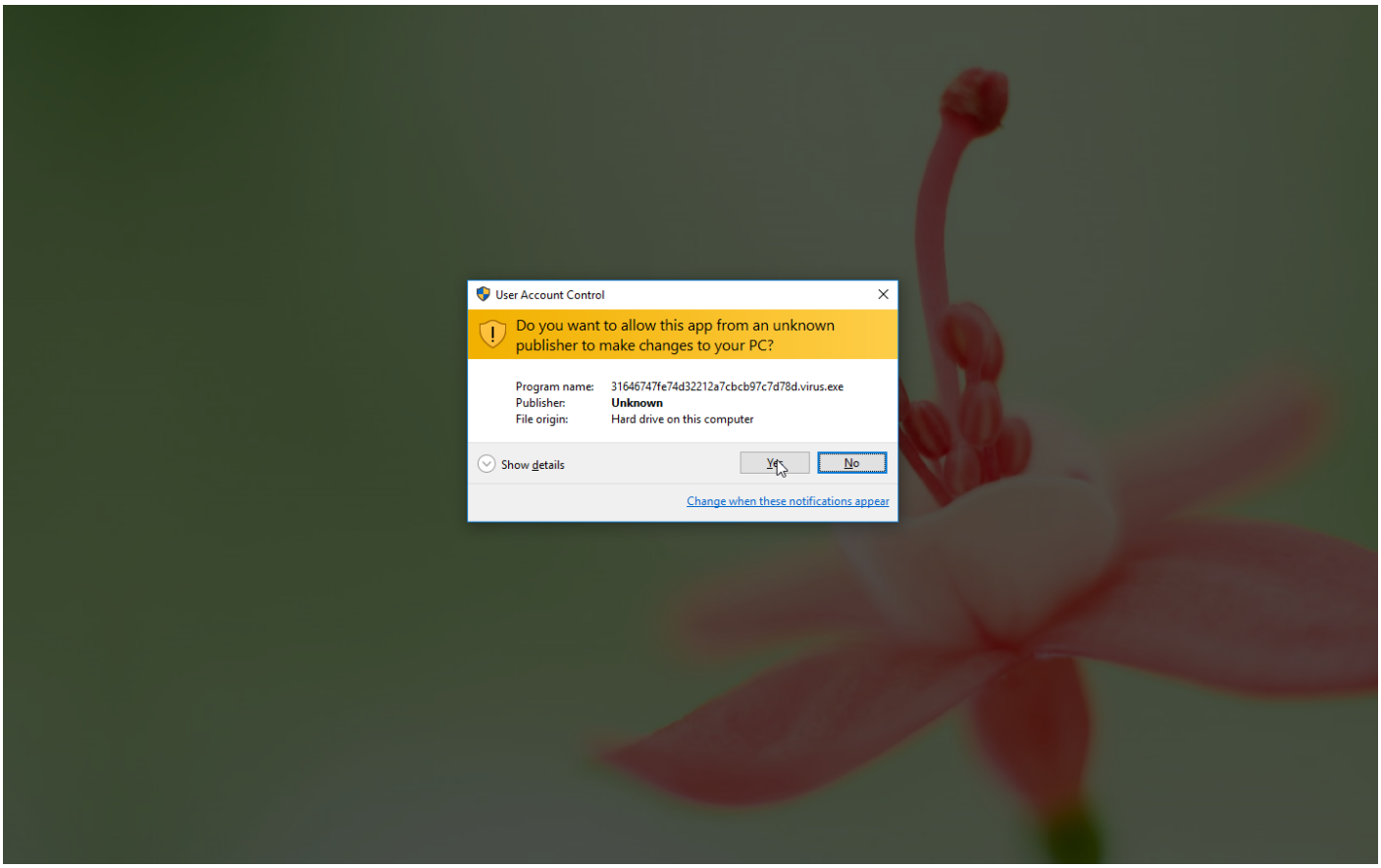
Sample Information

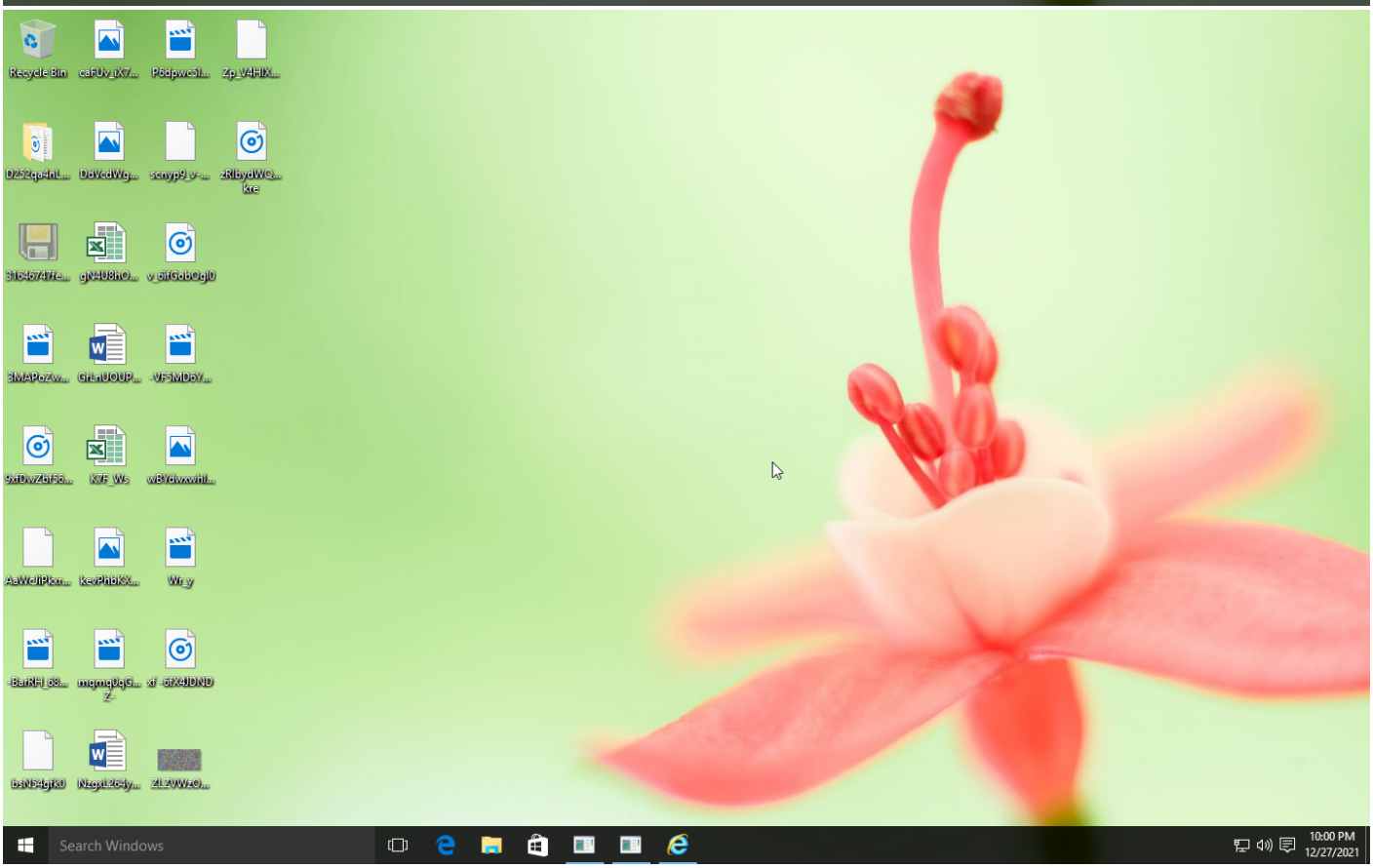
ID	#3193620
MD5	31646747fe74d32212a7cbcb97c7d78d
SHA1	62df758f397934053749ee38416a74f81a6d8ed6
SHA256	02bcb080116ab55475edbcd1293246a0e5d8894793ee9e699db805bff2935408
SSDeep	6144:EBGT3isLw0aTaB2Wc/Kimyj3OAHgAdHrlwZ0:EBGTSsLw0aTaB2Wc/jmyjNAAdHeZ
ImpHash	39de84e7a601fa8861e0e6a8c8b0a138
File Name	31646747fe74d32212a7cbcb97c7d78d.virus.exe
File Size	331.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-12-27 22:59 (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
Search Windows
9:59 PM
12/27/2021





Screenshots truncated

NETWORK

General

9.58 KB total sent

1503.13 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

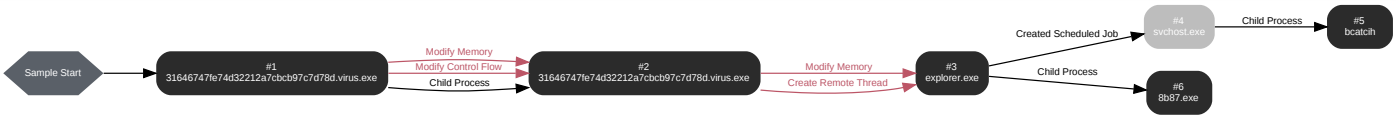
15 sessions, 9.58 KB sent, 1503.13 KB received

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: 31646747fe74d32212a7cbcb97c7d78d.virus.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 60131, Reason: Analysis Target
Unmonitor End Time	End Time: 86836, Reason: Terminated
Monitor duration	26.70s
Return Code	0
PID	3504
Parent PID	1560
Bitness	32 Bit

Host Behavior

Type	Count
Module	51
File	6
Environment	1
System	249
Window	1
Process	1
-	3
-	5

Process #2: 31646747fe74d32212a7cbcb97c7d78d.virus.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 78037, Reason: Child Process
Unmonitor End Time	End Time: 97263, Reason: Terminated
Monitor duration	19.23s
Return Code	0
PID	3640
Parent PID	3504
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\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0xc8c	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0xc8c	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0xc8c	0x227008(2256904)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0xc8c / 0x880	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: 92193, Reason: Injection
Unmonitor End Time	End Time: 301837, Reason: Terminated by Timeout
Monitor duration	209.64s
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\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0x880	0x2290000(36241408)	0x5000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0x880	0x400000(4194304)	0x16000	✓	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe	0x880	0x401930(4200752)	-	✓	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	331.50 KB	02bcb080116ab55475edbcd1293246a0e5d8894793ee9e699db805bff2935408	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.exe	1457.50 KB	b05eb68b03bca1e874e13403b0d0b57f4d76b70383b25be097b6fac78a1da3b5	✗

Host Behavior

Type	Count
Module	43
System	28829
Process	8680
Mutex	1
Registry	2
File	37
User	1
COM	1

Network Behavior

Type	Count
HTTP	15
TCP	15

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: 128580, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 301837, Reason: Terminated by Timeout
Monitor duration	173.26s
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: 138634, Reason: Child Process
Unmonitor End Time	End Time: 301837, Reason: Terminated by Timeout
Monitor duration	163.20s
Return Code	Unknown
PID	2356
Parent PID	860
Bitness	32 Bit

Host Behavior

Type	Count
Module	7
File	3
Environment	1

Process #6: 8b87.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\8b87.exe
Command Line	C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.exe
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 183096, Reason: Child Process
Unmonitor End Time	End Time: 301837, Reason: Terminated by Timeout
Monitor duration	118.74s
Return Code	Unknown
PID	4920
Parent PID	1560
Bitness	64 Bit

Host Behavior

Type	Count
Module	69
System	3
Environment	1
-	8
File	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
02bcb080116ab55475edbcd1293246a0e5d8894793ee9e699db805bff2935408	C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	331.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	MALICIOUS
b05eb68b03bca1e874e13403b0d0b57f4d76b70383b25be097b6fac78a1da3b5	C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.exe	Downloaded File	1457.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe	Sample File	Access, Delete	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	Access, Write, Delete, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Access, Delete	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\8B87.tmp	Accessed File	Access, Delete, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.exe	Downloaded File	Access, Write, Create	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-data-coin-11.com	-	5.188.89.48	-	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	5.188.89.48	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
5.188.89.48	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	31646747fe74d32212a7cbcb97c7d78d.virus.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	31646747fe74d32212a7cbcb97c7d78d.virus.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
31646747fe74d32212a7cbcb97c7d78d.virus.exe	"C:\Users\RDhJ0CNFevzX\Desktop\31646747fe74d32212a7cbcb97c7d78d.virus.exe"	MALICIOUS
8b87.exe	C:\Users\RDHJ0C~1\AppData\Local\Temp\8B87.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.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