

MALICIOUS

Classifications: Downloader Injector

Threat Names: SmokeLoader Mal/HTMLGen-A

Verdict Reason: -

Sample Type	Windows Exe (x86-32)
File Name	a7444553f8a8fe2702b6fd48008d6605.virus.exe
ID	#3275301
MD5	a7444553f8a8fe2702b6fd48008d6605
SHA1	f6d3d6ccf728ae7ab39b7e29f21ae5bcc7fce98b
SHA256	ba5303301925a877689b30efc36f872564f06906b2a61d7c3a7c955b0587d4f8
File Size	277.00 KB
Report Created	2022-01-13 20:25 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 25 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	3	Downloader
<ul style="list-style-type: none"> • 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) a7444553f8a8fe2702b6fd48008d6605.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	-
<ul style="list-style-type: none"> • (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\lbcatchi". 				
4/5	Reputation	Contacts known malicious URL	3	-
<ul style="list-style-type: none"> • Reputation analysis labels the URL "host-data-coin-11.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "185.112.83.96/build_dl" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "file-coin-host-12.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". 				
4/5	Injection	Writes into the memory of another process	1	Injector
<ul style="list-style-type: none"> • (Process #2) a7444553f8a8fe2702b6fd48008d6605.virus.exe modifies memory of (process #3) explorer.exe. 				
4/5	Injection	Modifies control flow of another process	1	Injector
<ul style="list-style-type: none"> • (Process #2) a7444553f8a8fe2702b6fd48008d6605.virus.exe creates thread in (process #3) explorer.exe. 				
2/5	Anti Analysis	Tries to detect debugger	1	-
<ul style="list-style-type: none"> • (Process #2) a7444553f8a8fe2702b6fd48008d6605.virus.exe tries to detect a debugger via API "NtQueryInformationProcess". 				
2/5	Hide Tracks	Deletes file after execution	2	-
<ul style="list-style-type: none"> • (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevz\appdata\roaming\lbcatchi". • (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevz\desktop\7444553f8a8fe2702b6fd48008d6605.virus.exe". 				
2/5	Anti Analysis	Delays execution	1	-
<ul style="list-style-type: none"> • (Process #3) explorer.exe has a thread which sleeps more than 5 minutes. 				
2/5	Task Scheduling	Schedules task	2	-
<ul style="list-style-type: none"> • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\lbcatchi", to be triggered by Logon. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\lbcatchi", to be triggered by Time. Task has been rescheduled by the analyzer. 				
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
<ul style="list-style-type: none"> • (Process #1) a7444553f8a8fe2702b6fd48008d6605.virus.exe modifies memory of (process #2) a7444553f8a8fe2702b6fd48008d6605.virus.exe. 				
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
<ul style="list-style-type: none"> • (Process #1) a7444553f8a8fe2702b6fd48008d6605.virus.exe alters context of (process #2) a7444553f8a8fe2702b6fd48008d6605.virus.exe. 				
1/5	Obfuscation	Reads from memory of another process	1	-
<ul style="list-style-type: none"> • (Process #1) a7444553f8a8fe2702b6fd48008d6605.virus.exe reads from (process #2) a7444553f8a8fe2702b6fd48008d6605.virus.exe. 				

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
<ul style="list-style-type: none"> (Process #1) a7444553f8a8fe2702b6fd48008d6605.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	-
<ul style="list-style-type: none"> (Process #3) explorer.exe enumerates running processes. 				
1/5	Mutex	Creates mutex	1	-
<ul style="list-style-type: none"> (Process #3) explorer.exe creates mutex with name "FE7F15060B875FB9FB2A49F08D5D03120C287F38". 				
1/5	Network Connection	Tries to connect using an uncommon port	1	-
<ul style="list-style-type: none"> (Process #3) explorer.exe tries to connect to TCP port 20000 at 185.112.83.96. 				
1/5	Execution	Executes itself	2	-
<ul style="list-style-type: none"> (Process #1) a7444553f8a8fe2702b6fd48008d6605.virus.exe executes a copy of the sample at C:\Users\RDhJOCNFevzX\Desktop\7444553f8a8fe2702b6fd48008d6605.virus.exe. (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJOCNFevzX\Desktop\7444553f8a8fe2702b6fd48008d6605.virus.exe. 				
1/5	Obfuscation	Resolves API functions dynamically	1	-
<ul style="list-style-type: none"> (Process #1) a7444553f8a8fe2702b6fd48008d6605.virus.exe resolves 41 API functions by name. 				

Mitre ATT&CK Matrix

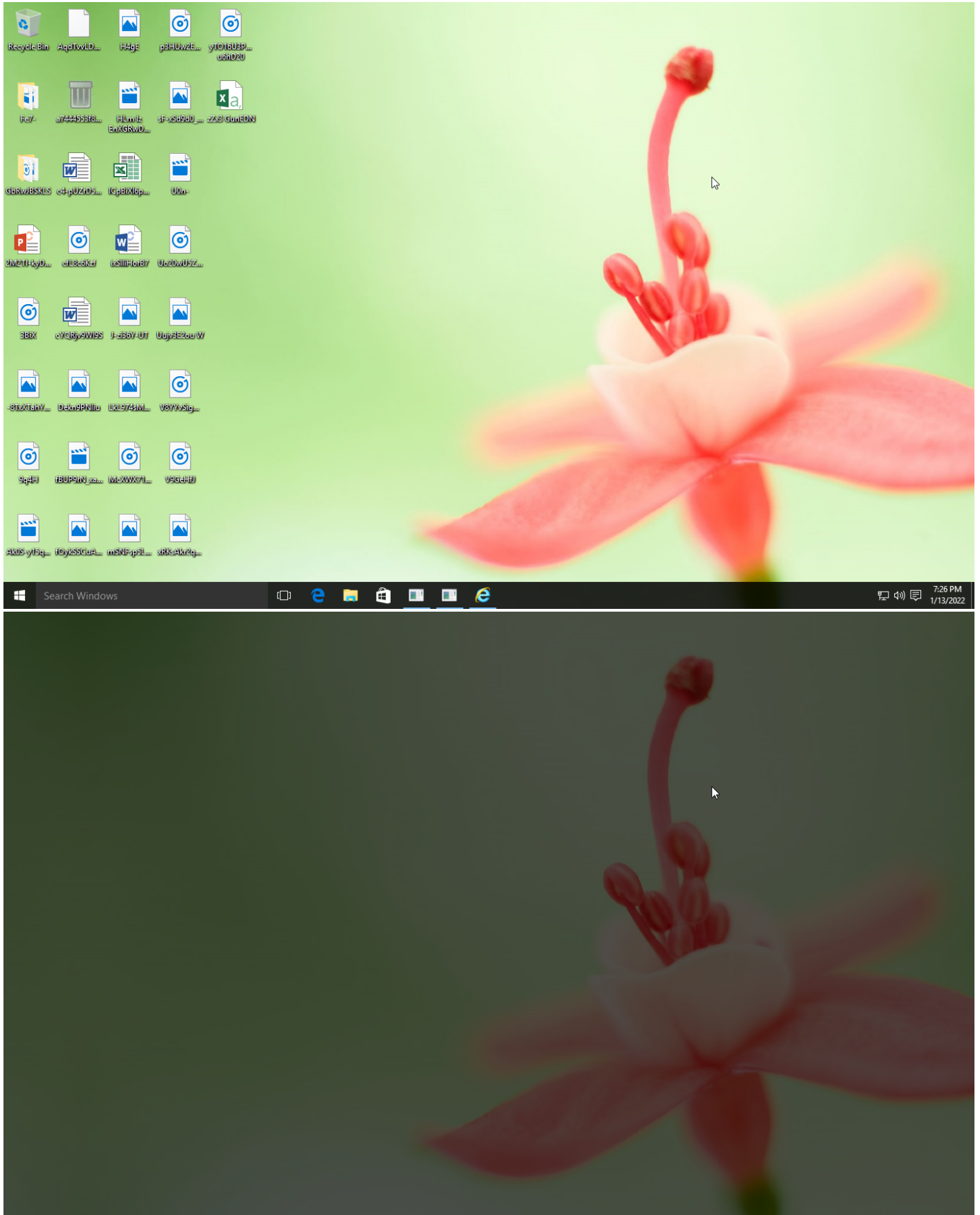
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery			#T1065 Uncommonly Used Port		
				#T1096 NTFS File Attributes							

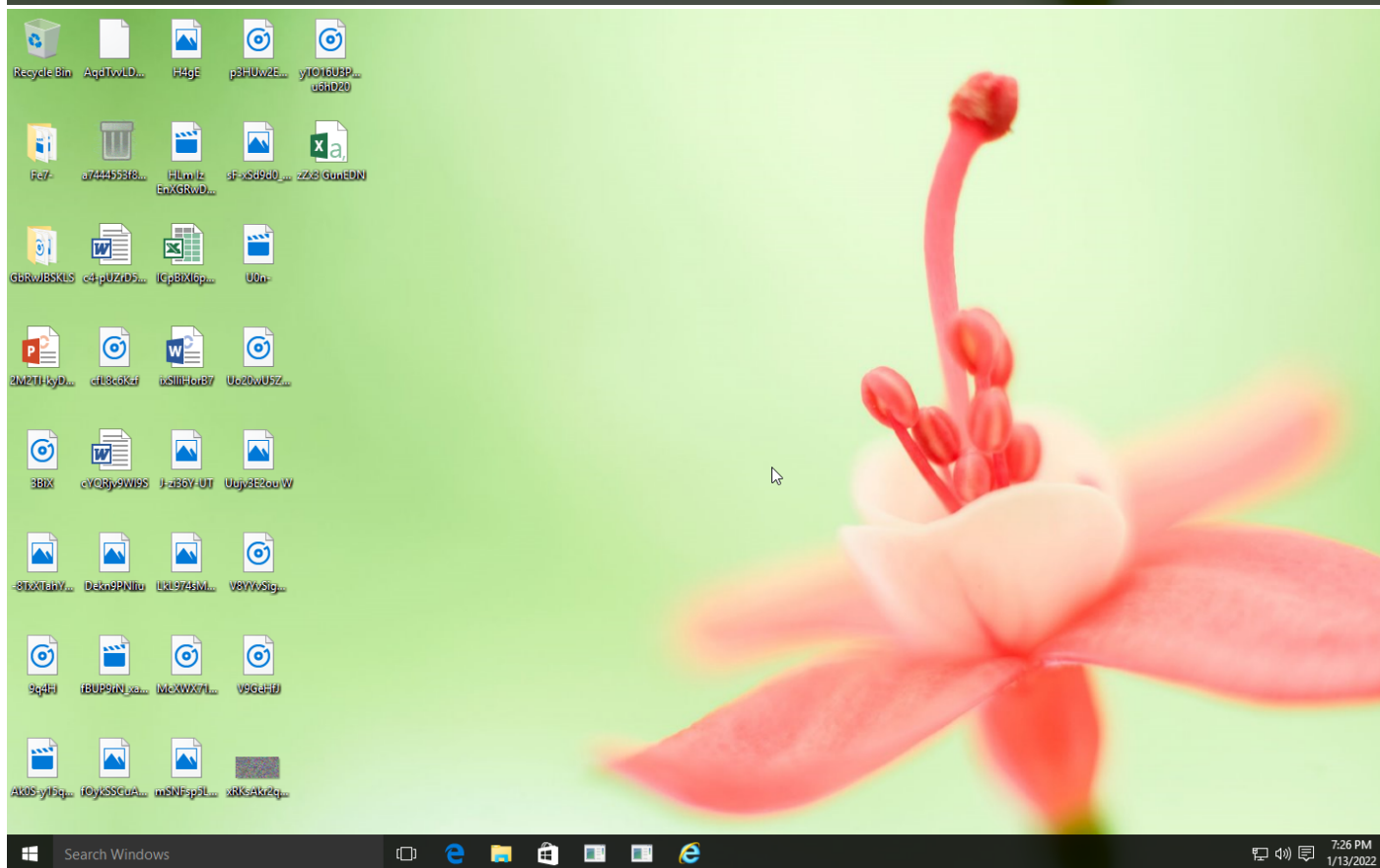
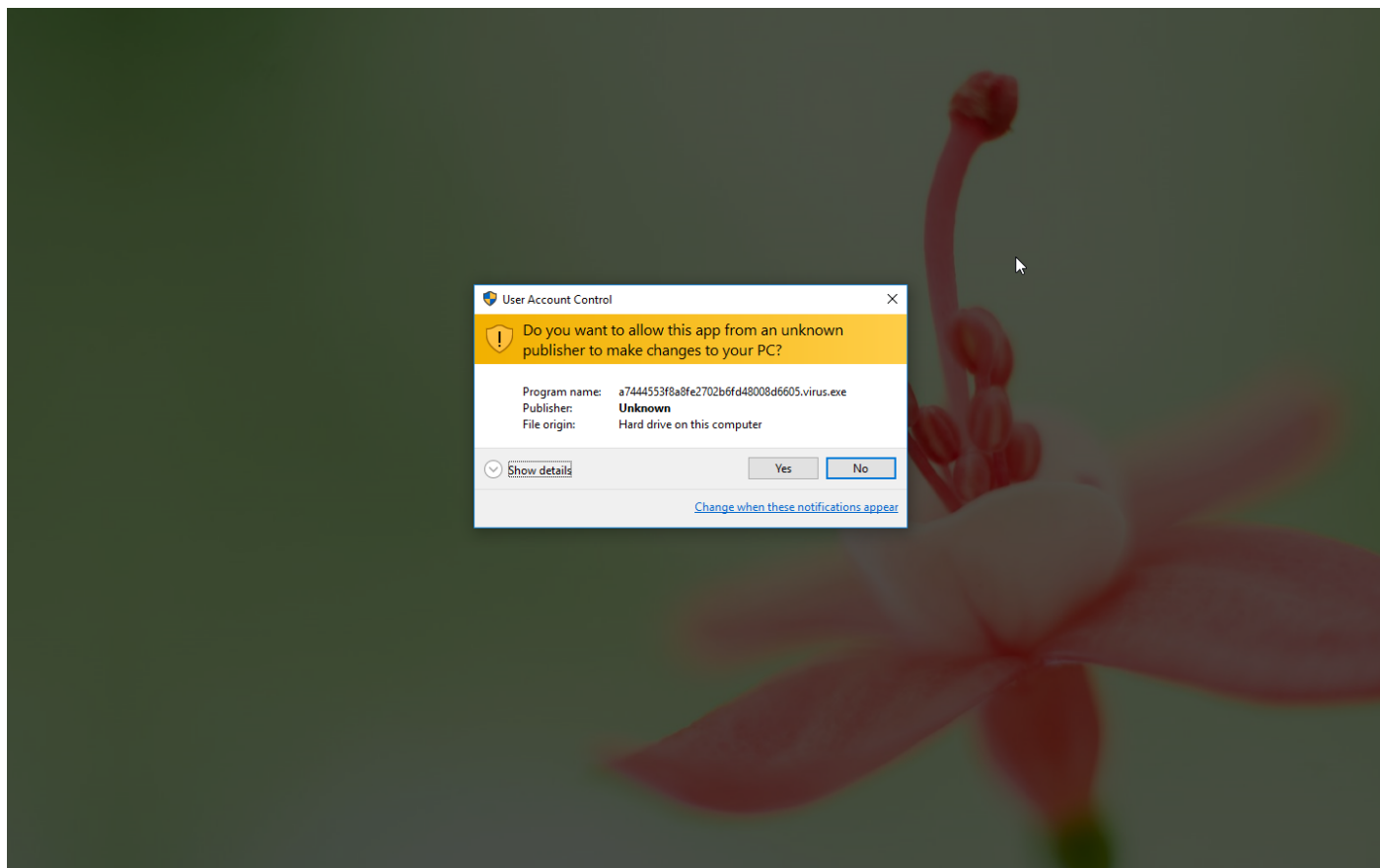
Sample Information

ID	#3275301
MD5	a7444553f8a8fe2702b6fd48008d6605
SHA1	f6d3d6ccf728ae7ab39b7e29f21ae5bcc7fce98b
SHA256	ba5303301925a877689b30efc36f872564f06906b2a61d7c3a7c955b0587d4f8
SSDeep	3072:AQAT6lATyGd4pXqYMER3QLSeuYerXcyGmofWrpxzbgqr: AQppHZQLSeNcbG/fuzbgwu
ImpHash	6d4af36ccbaddaffd179ef41d42df9cf
File Name	a7444553f8a8fe2702b6fd48008d6605.virus.exe
File Size	277.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-01-13 20:25 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	5
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





Screenshots truncated

NETWORK

General

9.70 KB total sent

4.56 KB total received

2 ports 80, 20000

3 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

3 URLs contacted, 3 servers

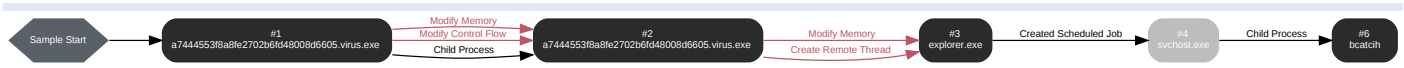
16 sessions, 9.70 KB sent, 4.56 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	host-data-coin-11.com/	-	-		0 bytes	NA
GET	185.112.83.96/build_dl	-	-		0 bytes	NA
POST	file-coin-host-12.com/	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: a7444553f8a8fe2702b6fd48008d6605.virus.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 71307, Reason: Analysis Target
Unmonitor End Time	End Time: 96718, Reason: Terminated
Monitor duration	25.41s
Return Code	0
PID	2012
Parent PID	1560
Bitness	32 Bit

Host Behavior

Type	Count
Module	72
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: a7444553f8a8fe2702b6fd48008d6605.virus.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 90440, Reason: Child Process
Unmonitor End Time	End Time: 112709, Reason: Terminated
Monitor duration	22.27s
Return Code	0
PID	764
Parent PID	2012
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\la7444553f8a8fe2702b6fd48008d6605.virus.exe	0x57c	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe	0x57c	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe	0x57c	0x33a008(3383304)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe	0x57c / 0xbcc	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: 106237, Reason: Injection
Unmonitor End Time	End Time: 312198, Reason: Terminated by Timeout
Monitor duration	205.96s
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\r\d\hj0cnfevz\desktop\7444553f8a8fe2702b6fd48008d6605.virus.exe	0xbcc	0x410000(4259840)	0x5000	✓	1
Modify Memory	#2: c:\users\r\d\hj0cnfevz\desktop\7444553f8a8fe2702b6fd48008d6605.virus.exe	0xbcc	0x420000(4325376)	0x16000	✓	1
Create Remote Thread	#2: c:\users\r\d\hj0cnfevz\desktop\7444553f8a8fe2702b6fd48008d6605.virus.exe	0xbcc	0x421930(4331824)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\r\d\hj0CNFevz\X\AppData\Roaming\lbcatch	277.00 KB	ba5303301925a877689b30efc36f872564f06906b2a61d7c3a7c955b0587d4f8	✗

Host Behavior

Type	Count
Module	43
System	33401
Process	4558
Mutex	1
Registry	2
File	35
User	1
COM	1

Network Behavior

Type	Count
HTTP	16
TCP	16

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: 143948, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 312198, Reason: Terminated by Timeout
Monitor duration	168.25s
Return Code	Unknown
PID	860
Parent PID	532
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: 153142, Reason: Child Process
Unmonitor End Time	End Time: 312198, Reason: Terminated by Timeout
Monitor duration	159.06s
Return Code	Unknown
PID	5072
Parent PID	860
Bitness	32 Bit

Host Behavior

Type	Count
Module	29
File	3
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ba5303301925a877689b30efc36f872564f06906b2a61d7c3a7c955b0587d4f8	C: \Users\RDhJ0CNFevzX\Desktop\44553f8a8fe2702b6fd48008d6605.virus.exe, C: \Users\RDhJ0CNFevzX\AppData\Roaming\bcatch	Sample File	277.00 KB	application/vnd.microsoft.portable-executable	Access, Delete, Create, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C: \Users\RDhJ0CNFevzX\Desktop\4444553f8a8fe2702b6fd48008d6605.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\bcatch	Sample File	Access, Delete, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatch.Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbf	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://host-data-coin-11.com	-	45.135.233.182	-	POST	MALICIOUS
http://185.112.83.96/build_dl	-	185.112.83.96	-	GET	MALICIOUS
http://file-coin-host-12.com	-	-	-	POST	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
host-data-coin-11.com	45.135.233.182	-	HTTP	CLEAN
file-coin-host-12.com	-	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.135.233.182	host-data-coin-11.com	Russia	DNS, HTTP, TCP	CLEAN
185.112.83.96	-	Russia	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	a7444553f8a8fe2702b6fd48008d6605.virus.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	a7444553f8a8fe2702b6fd48008d6605.virus.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN

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

Process

Process Name	Commandline	Verdict
a7444553f8a8fe2702b6fd48008d6605.virus.exe	"C:\Users\RDhJ0CNFevzX\Desktop\la7444553f8a8fe2702b6fd48008d6605.virus.exe"	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
bcatch	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatch	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