MALICIOUS

Classifications: Injector | Downloader

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe**
ID	#5059311
MD5	785d9d53c4b721385e9e5f51a4846791
SHA1	751b17ab9fae896ed414f42dacd885bd75a83f46
SHA256	6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f
File Size	338.50 KB
Report Created	2022-08-04 12:49 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (21 rules, 28 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 "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe. • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump 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) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.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) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe. • Rule "VMProcessNames" from ruleset "Generic" has matched on the function strings for (process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe. • Rule "VMModuleNames" from ruleset "Generic" has matched on the function strings for (process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.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\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe modifies memory of (process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe alters context of (process #2) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.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.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe reads from (process #1) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.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	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) 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe resolves 43 API functions by name. • (Process #6) bcatcih resolves 43 API functions by name.			

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

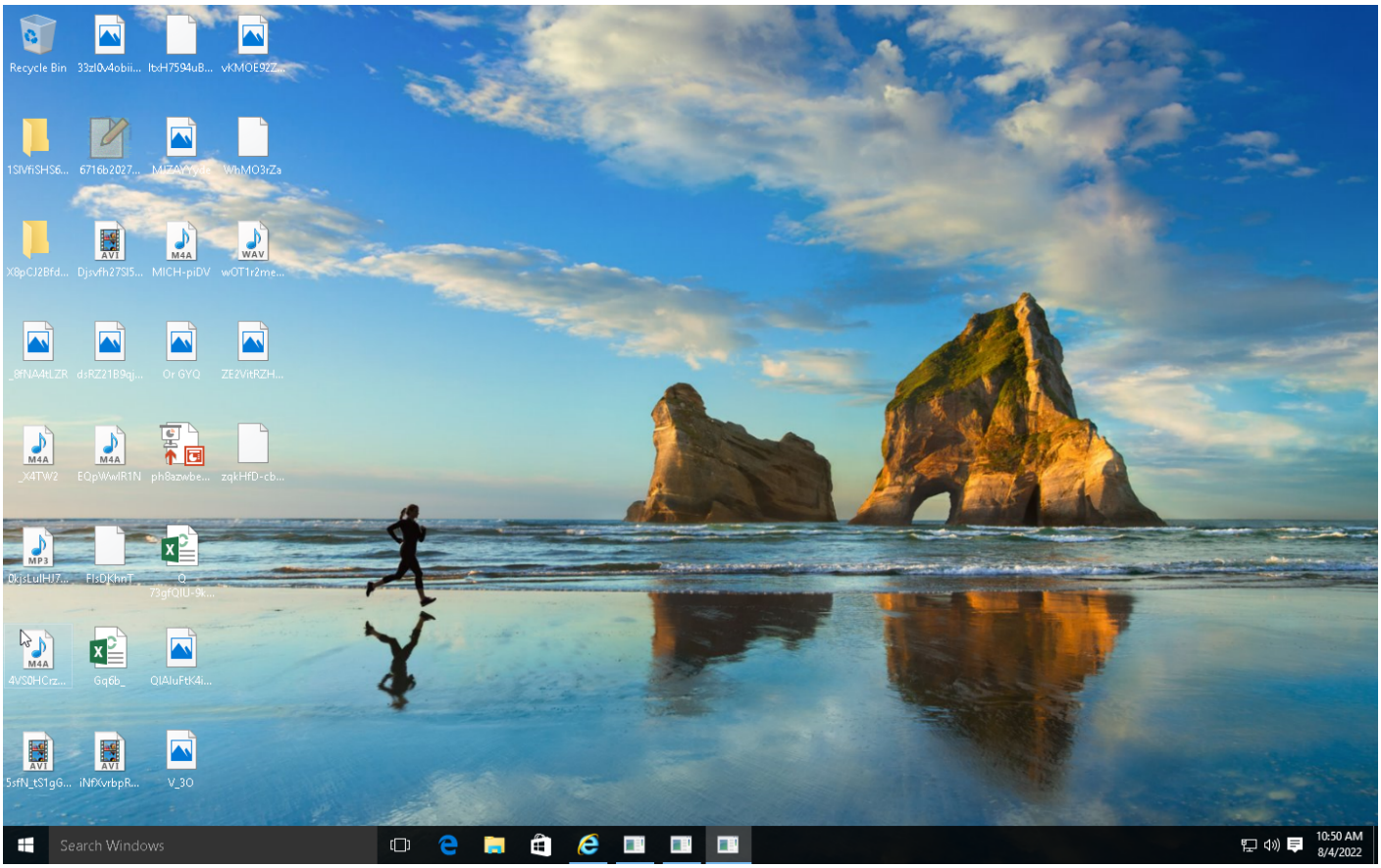
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
				#T1096 NTFS File Attributes					#T1105 Remote File Copy		

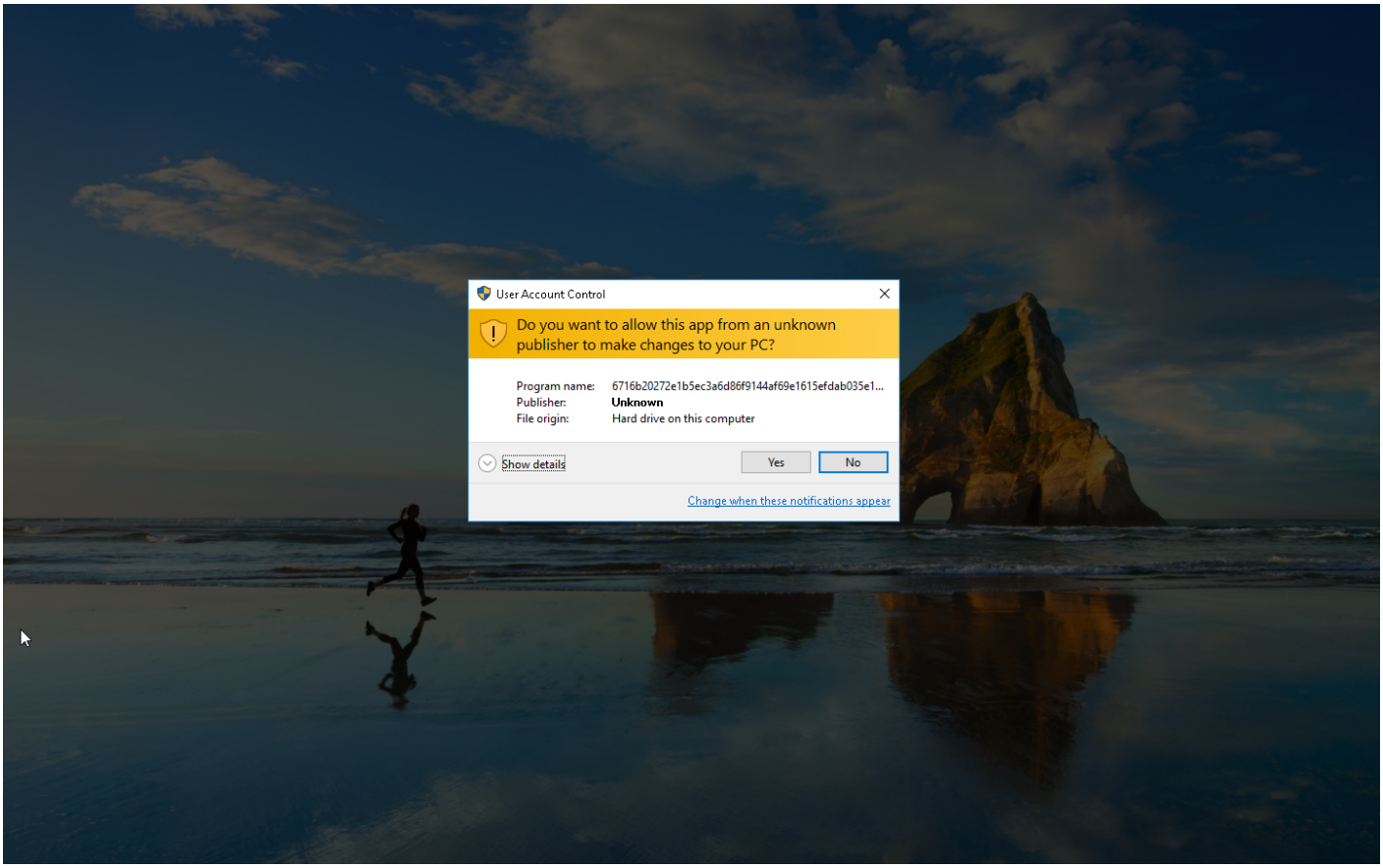
Sample Information

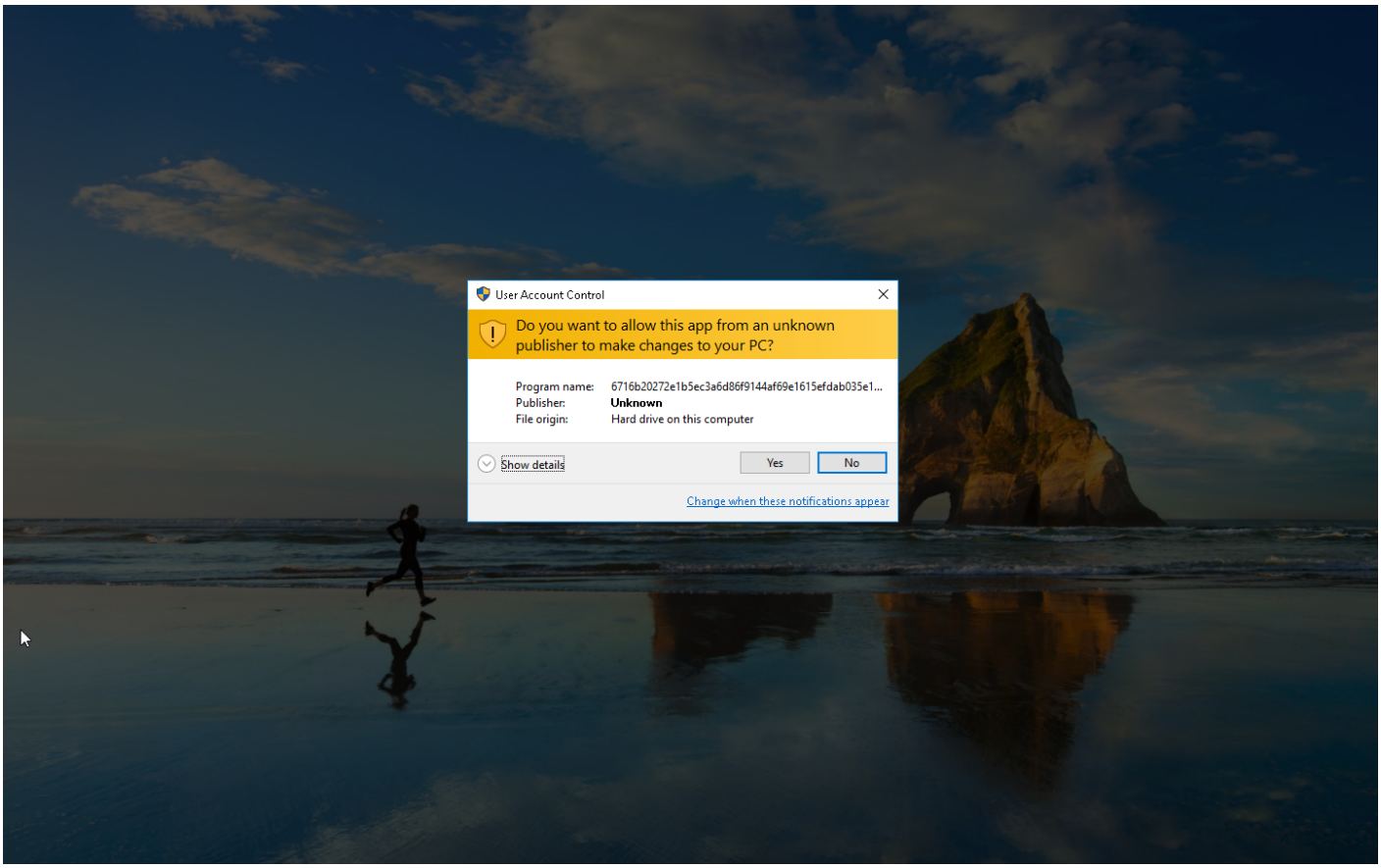
ID	#5059311
MD5	785d9d53c4b721385e9e5f51a4846791
SHA1	751b17ab9fae896ed414f42dacd885bd75a83f46
SHA256	6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f
SSDeep	6144:kbielRAT0GZkAMOHG/HBCssiXE8du+9W0U:kmehKkZOHGfBCsG29W
ImpHash	9da6af138aaaf087a1ce609a65e93d9a
File Name	6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe
File Size	338.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

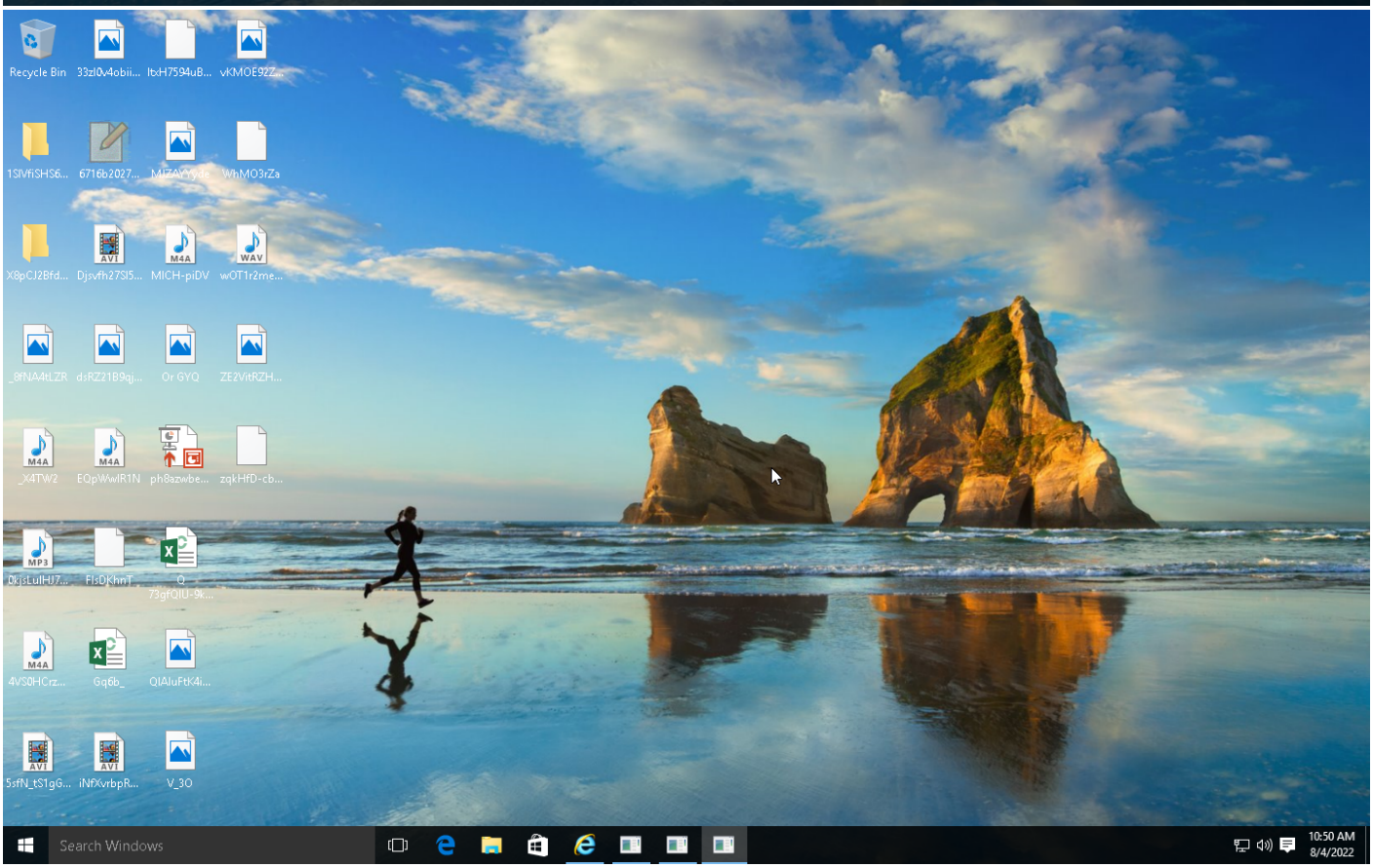
Analysis Information

Creation Time	2022-08-04 12:49 (UTC+2)
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	6


Recycle Bin
Search Windows
10:50 AM
8/4/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e1...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

3.01 KB total sent

1.60 KB total received

2 ports 80, 53

2 contacted IP addresses

1 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

4 sessions, 2.95 KB sent, 1.52 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://host-file-host6.com	-	-		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

BEHAVIOR

Process Graph

Process #1: 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 63251, Reason: Analysis Target
Unmonitor End Time	End Time: 92026, Reason: Terminated
Monitor duration	28.77s
Return Code	0
PID	4916
Parent PID	1972
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	338.50 KB	6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f	✖

Host Behavior

Type	Count
Module	76
File	6
Environment	1
Window	1
Process	1
-	3
-	5

Process #2: 6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 84815, Reason: Child Process
Unmonitor End Time	End Time: 107085, Reason: Terminated
Monitor duration	22.27s
Return Code	0
PID	4956
Parent PID	4916
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\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1338	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1338	0x401000(4198400)	0x7200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1338	0x3b9008(3903496)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1338 / 0x1360	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: 100541, Reason: Injection
Unmonitor End Time	End Time: 303818, Reason: Terminated by timeout
Monitor duration	203.28s
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\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1360	0x550000(5570560)	0x5000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1360	0x560000(5636096)	0x16000	✔	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	0x1360	0x561930(5642544)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	338.50 KB	6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f	✖

Host Behavior

Type	Count
Module	27
System	10221
Process	1753
Mutex	1
Registry	2
File	17
User	1
COM	1

Network Behavior

Type	Count
HTTP	4

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: 139526, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 303818, Reason: Terminated by timeout
Monitor duration	164.29s
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: 150306, Reason: Child Process
Unmonitor End Time	End Time: 303818, Reason: Terminated by timeout
Monitor duration	153.51s
Return Code	Unknown
PID	3576
Parent PID	864
Bitness	32 Bit

Host Behavior

Type	Count
Module	74
File	6
Environment	1
Window	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f	C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	338.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
f02d38c2314903b79375250343ff0237e1f3d5ff0abc6a7e84cb3eac13d96a485	-	Downloaded File	24 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	Sample File, Accessed File, VM File	Access, Delete	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Access, Delete	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa	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

Domain

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

IP

IP Address	Domains	Country	Protocols	Verdict
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	access	explorer.exe	CLEAN

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

Process

Process Name	Commandline	Verdict
6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	"C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe"	MALICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe	"C:\Users\RDhJ0CNFevzX\Desktop\6716b20272e1b5ec3a6d86f9144af69e1615efdab035e130b654757b36e8b84f.exe"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (6)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Generic	VMDeviceStrings	VM detection via known device names	Function Strings	-	-	3/5
Generic	VMProcessNames	VM detection via known process names	Function Strings	-	-	3/5
Generic	VMModuleNames	VM detection via known module names	Function Strings	-	-	3/5

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