MALICIOUS

Classifications: Downloader | Injector

Threat Names: SmokeLoader | Mal/Generic-S | Mal/HTMLGen-A | Generic.Andromeda.79093CCD | Gen:Variant.Razy.655877

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**toolspab3.exe**
ID	#1221062
MD5	1a430b2cbf785427c87c48d29a1a8c0f
SHA1	e9b392c34c1bf0e42599bb561f111e3bcea7b3d9
SHA256	1d1fc9d23aa14b4f484fb86c173c94084bc14a9f551747b6e06366649a229af5
File Size	329.00 KB
Report Created	2021-12-01 08:35 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (19 rules, 25 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Downloader
	• 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) toolspab3.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) toolspab3.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	2	-
	• 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 "file-coin-host-12.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected a memory dump of (process #1) toolspab3.exe as "Generic.Andromeda.79093CCD". • Built-in AV detected a memory dump of (process #2) toolspab3.exe as "Gen:Variant.Razy.655877".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) toolspab3.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\toolspab3.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	-
	• (Process #1) toolspab3.exe modifies memory of (process #2) toolspab3.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) toolspab3.exe alters context of (process #2) toolspab3.exe.			
2/5	Task Scheduling	Schedules task	2	-

Score	Category	Operation	Count	Classification
	• 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) toolspab3.exe reads from (process #2) toolspab3.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) toolspab3.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	Execution	Executes itself	2	-
	• (Process #1) toolspab3.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe. • (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) toolspab3.exe resolves 39 API functions by name.			

Mitre ATT&CK Matrix

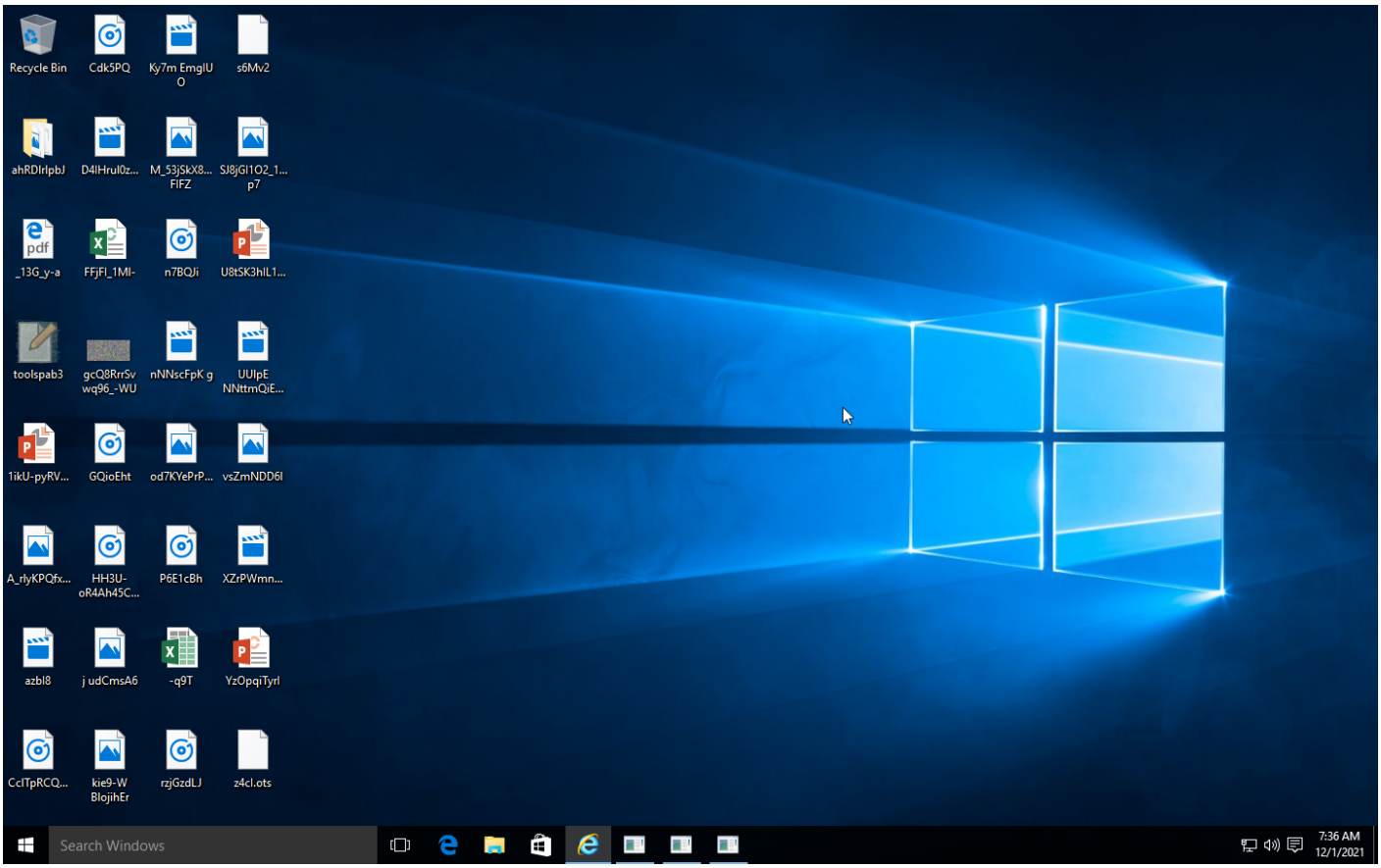
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery					
				#T1096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

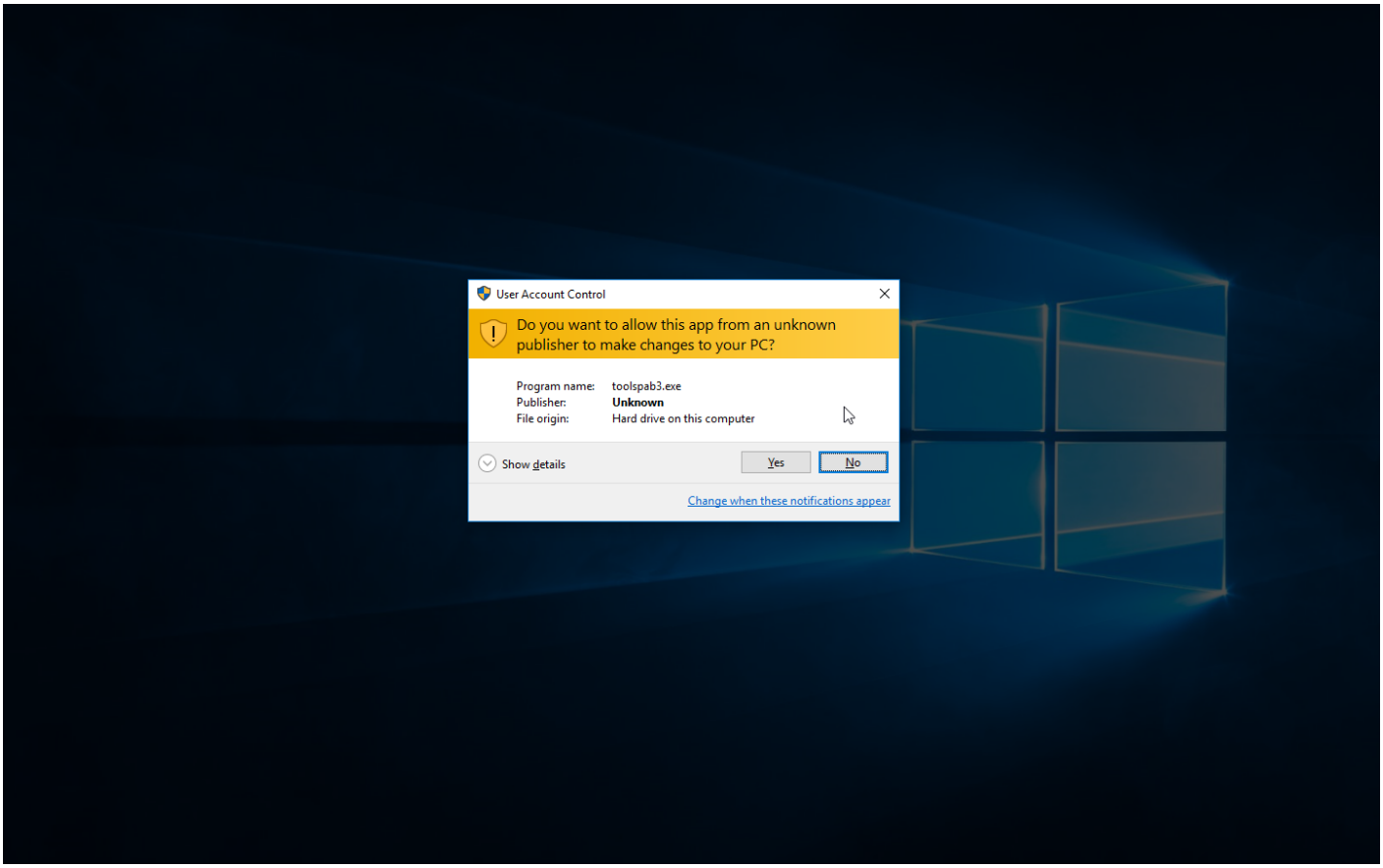
Sample Information

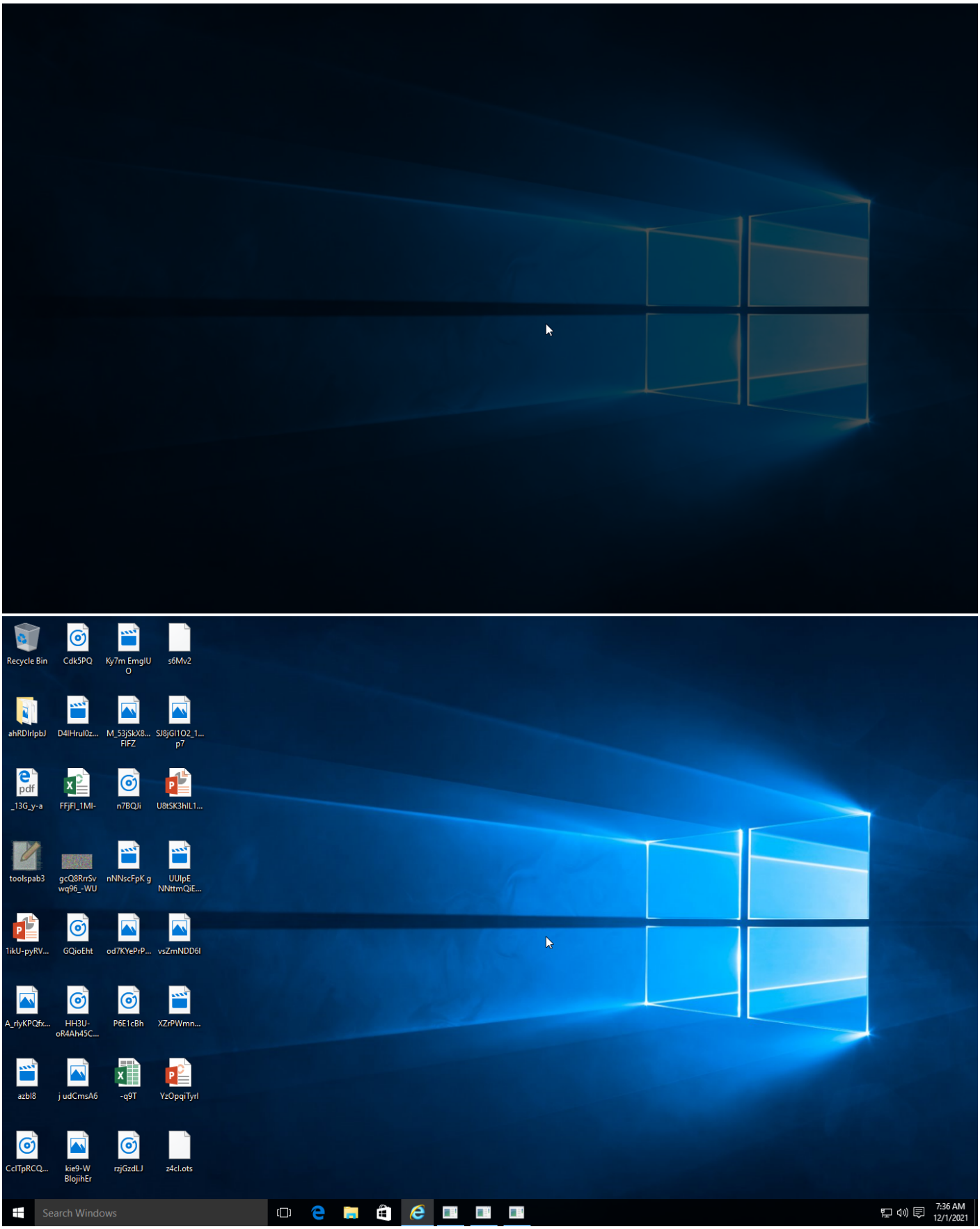
ID	#1221062
MD5	1a430b2cbf785427c87c48d29a1a8c0f
SHA1	e9b392c34c1bf0e42599bb561f111e3bcea7b3d9
SHA256	1d1fc9d23aa14b4f484fb86c173c94084bc14a9f551747b6e06366649a229af5
SSDeep	6144:MaXePnFllS35U3jiXtHAt7ewOljc4hDxElcyG+V5:MaqllS35U3jiXtHAt7XOlw4jElcyG
ImpHash	eddec1d3c2023ed0e1e37ce0535d3b62
File Name	toolspab3.exe
File Size	329.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-12-01 08:35 (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	3
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2


Recycle Bin
Cdk5PQ
Ky7m EmgIU O
s6Mv2
ahRDIrlpbJ
D4lHrul0z...
M_53jSkX8... FIFZ
SJ8jGI1O2_1... p7
_13G_y-a
FFjFl_1MI-
n7BQJi
U8tSK3hIL1...
toolspab3
gcQ8RrrSv wq96_-WU
nNNscFpK g
UUlpE NNttmQiE...
1ikU-pyRV...
GQioEht
od7KYePrP...
vsZmNDD6I
A_rlyKPQfx...
HH3U-oR4Ah45C...
P6E1cBh
XZrPWmn...
azbl8
j udCmsA6
-q9T
YzOpqiTyrl
CcITpRCQ...
kie9-W BlojihEr
rzjGzdLJ
z4cl.ots
Search Windows
7:36 AM
12/1/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: toolspab3.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

2.54 KB total sent

1.11 KB total received

1 ports 80

2 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

2 URLs contacted, 2 servers

5 sessions, 2.54 KB sent, 1.11 KB received

HTTP Requests

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

BEHAVIOR

Process Graph

Process #1: toolspab3.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\toolspab3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 65617, Reason: Analysis Target
Unmonitor End Time	End Time: 97586, Reason: Terminated
Monitor duration	31.97s
Return Code	0
PID	3092
Parent PID	1636
Bitness	32 Bit

Host Behavior

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

Process #2: toolspab3.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\toolspab3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 89935, Reason: Child Process
Unmonitor End Time	End Time: 108986, Reason: Terminated
Monitor duration	19.05s
Return Code	0
PID	4884
Parent PID	3092
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\toolspab3.exe	0x12c8	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\toolspab3.exe	0x12c8	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\toolspab3.exe	0x12c8	0x38f008(3731464)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\toolspab3.exe	0x12c8 / 0x1310	0x772d8fe0(1999474656)	-	✓	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: 104393, Reason: Injection
Unmonitor End Time	End Time: 308300, Reason: Terminated by Timeout
Monitor duration	203.91s
Return Code	Unknown
PID	1636
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\toolspab3.exe	0x1310	0x410000(4259840)	0x5000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\toolspab3.exe	0x1310	0x420000(4325376)	0x16000	✓	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\toolspab3.exe	0x1310	0x421930(4331824)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	329.00 KB	1d1fc9d23aa14b4f484fb86c173c94084bc14a9f551747b6e06366649a229af5	✗

Host Behavior

Type	Count
Module	25
System	10629
Process	2561
Mutex	1
Registry	2
File	17
User	1
COM	1

Network Behavior

Type	Count
HTTP	5
TCP	5

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: 152579, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 308300, Reason: Terminated by Timeout
Monitor duration	155.72s
Return Code	Unknown
PID	836
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: 162905, Reason: Child Process
Unmonitor End Time	End Time: 308300, Reason: Terminated by Timeout
Monitor duration	145.40s
Return Code	Unknown
PID	2232
Parent PID	836
Bitness	32 Bit

Host Behavior

Type	Count
Module	7
File	3
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1d1fc9d23aa14b4f484fb86c173c94084bc14a9f551747b6e06366649a229af5	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih, C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe	Sample File	329.00 KB	application/vnd.microsoft.portable-executable	Delete, Create, Access, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe	Sample File	Delete, Access	CLEAN
apfHQ	Accessed File	Access	CLEAN
C:\Windows\system32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	Sample File	Delete, Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier	Accessed File	Delete, 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-data-coin-11.com	-	95.213.165.249	-	POST	MALICIOUS
http://file-coin-host-12.com	-	-	-	POST	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
host-data-coin-11.com	95.213.165.249	-	HTTP	CLEAN
file-coin-host-12.com	-	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
95.213.165.249	host-data-coin-11.com	Russia	TCP, DNS, HTTP	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	toolspab3.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	toolspab3.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
toolspab3.exe	"C:\Users\RDhJ0CNFevzX\Desktop\toolspab3.exe"	MALICIOUS
bcatcih	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5
Malware	SmokeLoaderStrings	SmokeLoader strings	Function Strings	function_strings_process_3.txt	Downloader	5/5

Antivirus (3)

File Type	Threat Name	File Name	Verdict
Memory Dump	Generic.Andromeda.79093CCD	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	MALICIOUS

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	4.3.1
Dynamic Engine Version	4.3.1 / 11/09/2021 04:55
Static Engine Version	4.3.1.0 / 2021-11-09 04:00:13
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.23 / 2021-11-15 15:11:35
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.24 / 2021-11-19 15:51:18
YARA Built-in Ruleset Version	4.3.1.20

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-12-01 04:59:37+00:00
Built-in AV Database Records	10594378

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