MALICIOUS

Classifications: Downloader, Injector

Threat Names: SmokeLoader, Mal/HTMLGen-A, Gen:Variant.Fragtor.35416, Generic.Andromeda.D4A614B0, Generic.Andromeda.79093CCD, Gen:Variant.Razy.655877

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe**
ID	#2921186
MD5	36f662b3c9a54c0c2427602f1463eb69
SHA1	7e46615097282ac51ef08d3e4ac7d65ce6684a07
SHA256	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed
File Size	185.50 KB
Report Created	2021-10-27 15:59 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (19 rules, 27 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Downloader
	• 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) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe modifies memory of (process #3) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #2) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe creates thread in (process #3) explorer.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected the sample itself as "Gen:Variant.Fragtor.35416". • Built-in AV detected a memory dump of (process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe as "Generic.Andromeda.D4A614B0". • Built-in AV detected a memory dump of (process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe as "Generic.Andromeda.79093CCD". • Built-in AV detected a memory dump of (process #2) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe as "Gen:Variant.Razy.655877".			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the URL "gejajoo7.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "sysaheu9.top/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #2) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.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\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
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.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe modifies memory of (process #2) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe alters context of (process #2) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe.			

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe reads from (process #2) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.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) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe. • (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe resolves 39 API functions by name.			
1/5	Network Connection	All network connection attempts failed	2	-
	• Host "gejajoo7.top" is unavailable. • Host "sysaheu9.top" is unavailable.			

Mitre ATT&CK Matrix

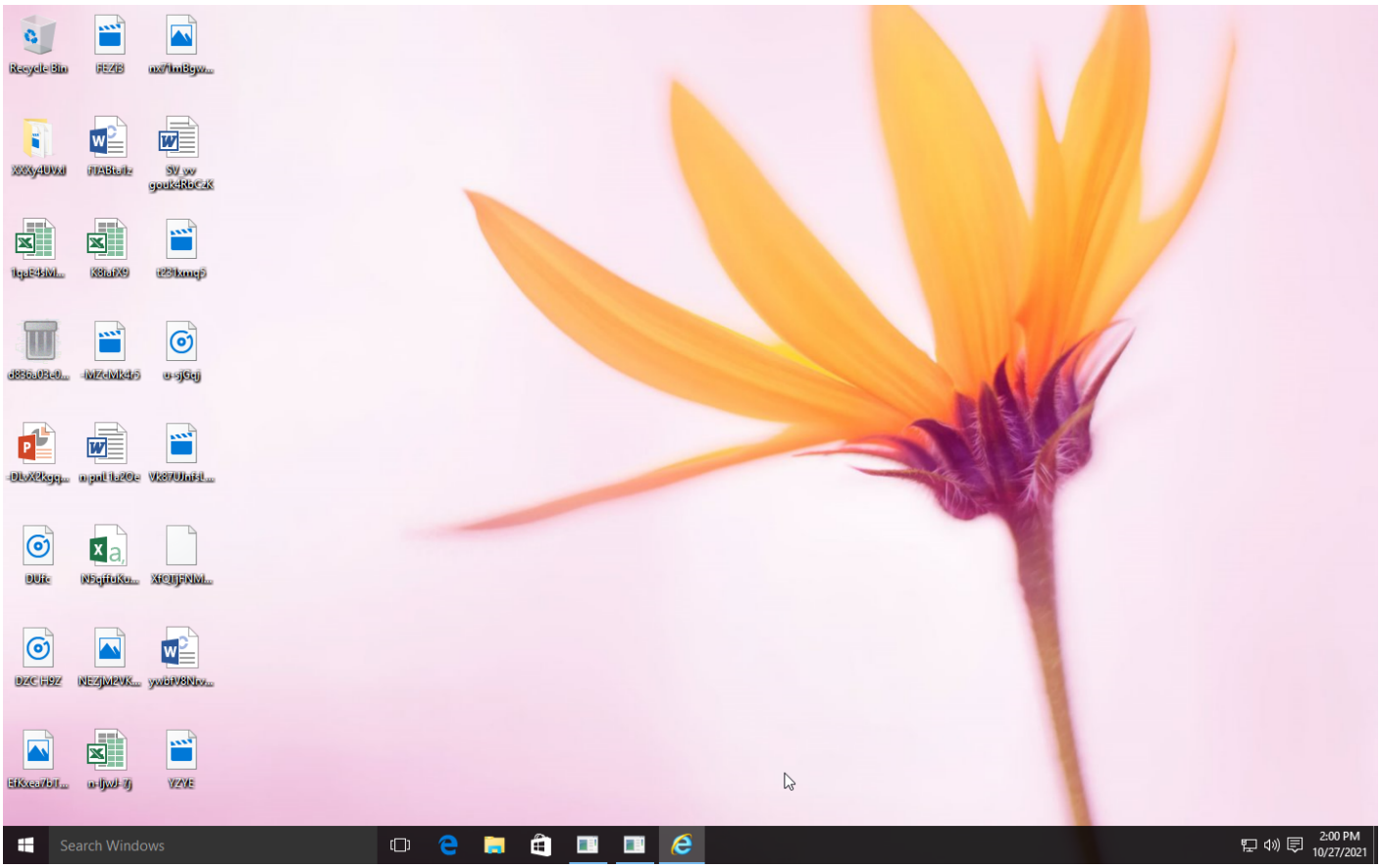
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1045 Software Packing		#T1057 Process Discovery					
				#T1096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

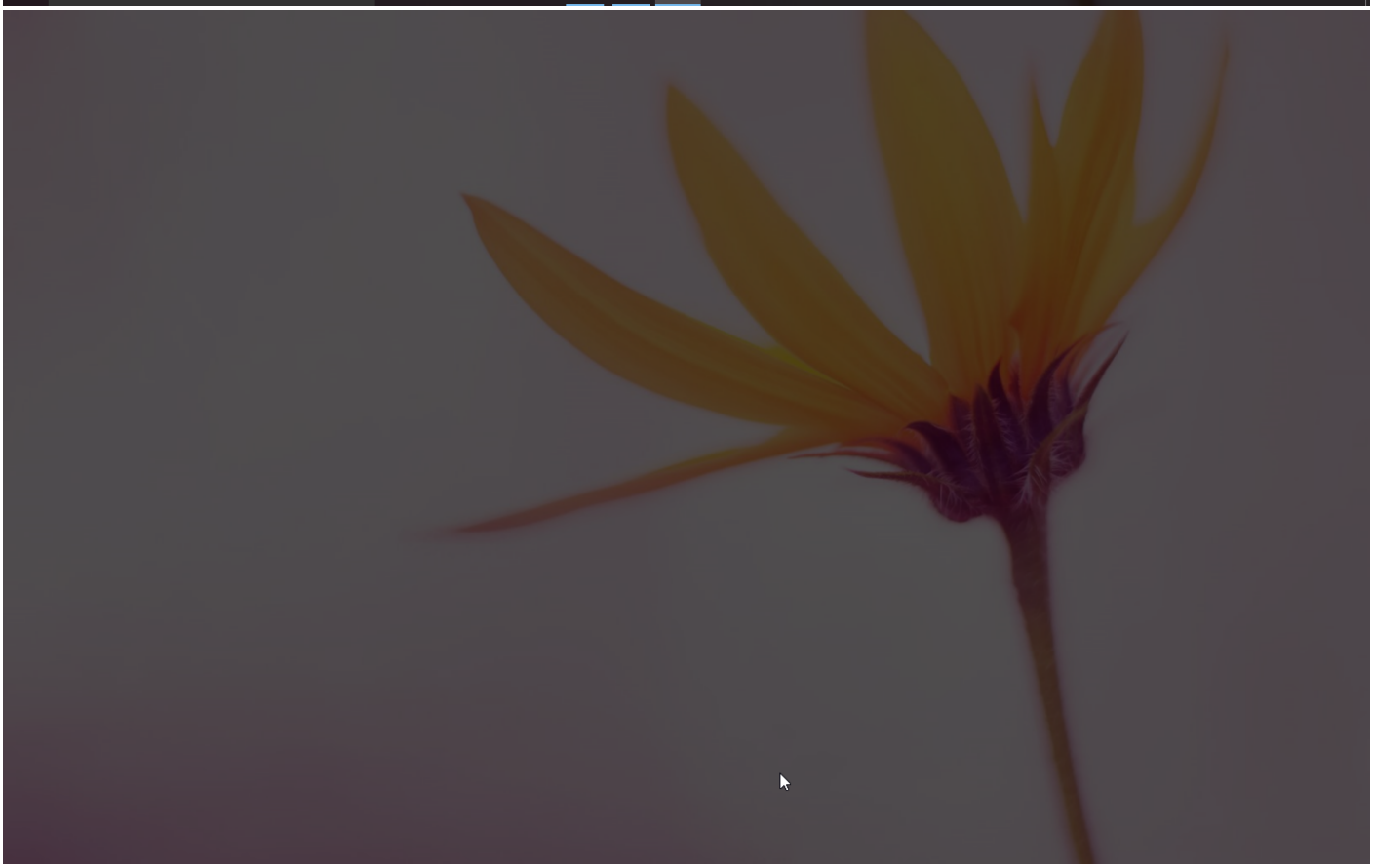
Sample Information

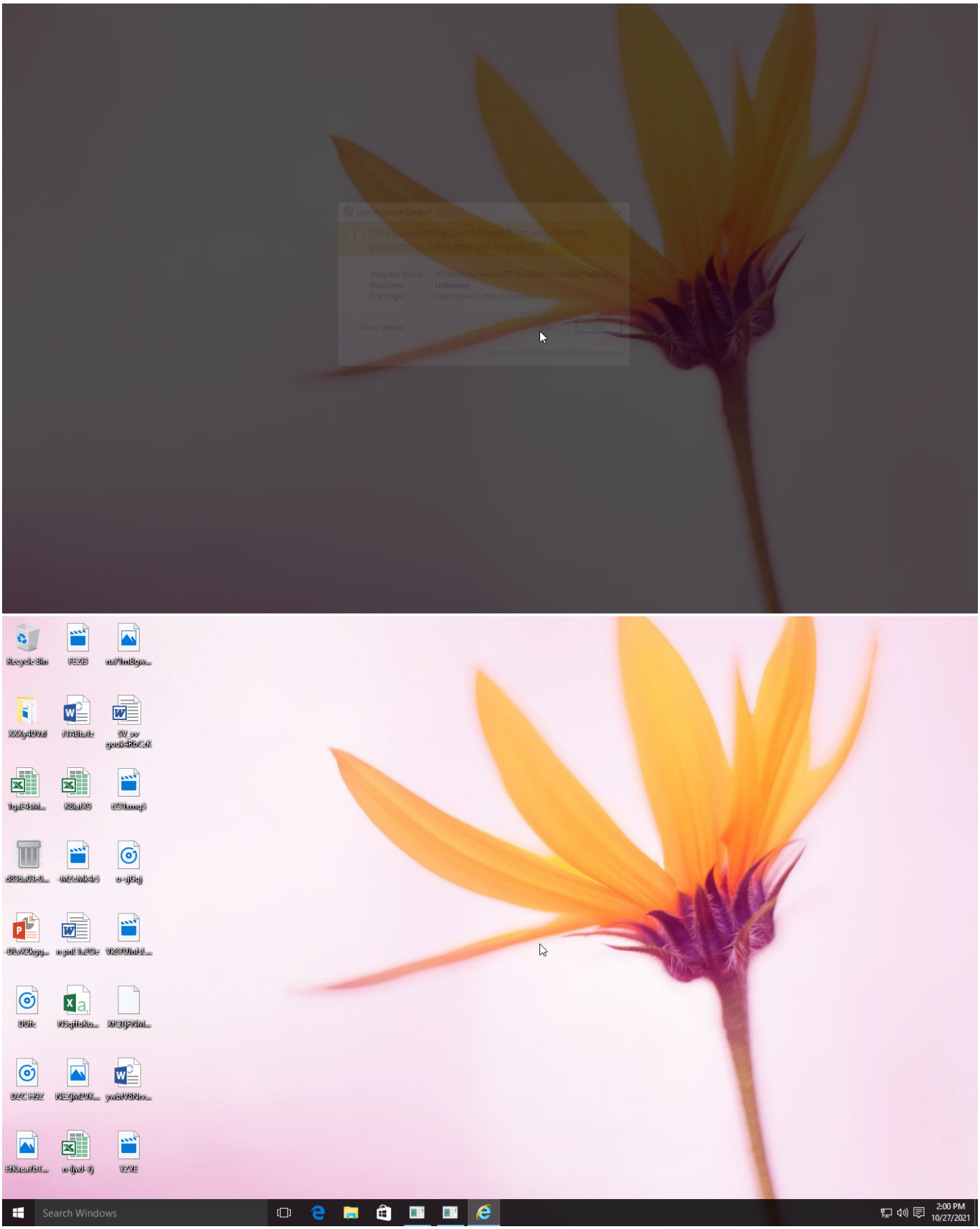
ID	#2921186
MD5	36f662b3c9a54c0c2427602f1463eb69
SHA1	7e46615097282ac51ef08d3e4ac7d65ce6684a07
SHA256	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed
SSDeep	3072:5+d4MmCHgQlJeblXMLQPAkilxUj3RMsOEd7lj/CrzeuVMO6P2+BwvHJ3/Rg:Ad4aHgaulXyQ4kicim9/C+ynVP
ImpHash	fa148d0c70a978454538a9c9c0513fc1
File Name	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe
File Size	185.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-10-27 15:59 (UTC+2)
Analysis Duration	00:03:55
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	6
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Search Windows
2:00 PM
10/27/2021





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 80

1 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

2 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	gejajoo7.top/	-	-		0 bytes	NA
POST	sysaheu9.top/	-	-		0 bytes	NA

BEHAVIOR

Process Graph

Process #1: d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 88142, Reason: Analysis Target
Unmonitor End Time	End Time: 125376, Reason: Terminated
Monitor duration	37.23s
Return Code	0
PID	3388
Parent PID	1600
Bitness	32 Bit

Host Behavior

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

Process #2: d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 115453, Reason: Child Process
Unmonitor End Time	End Time: 143378, Reason: Terminated
Monitor duration	27.93s
Return Code	0
PID	1496
Parent PID	3388
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\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0x714	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0x714	0x401000(4198400)	0x7200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0x714	0x3b1008(3870728)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0x714 / 0xd10	0x77968fe0(2006355936)	-	✓	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: 135061, Reason: Injection
Unmonitor End Time	End Time: 323864, Reason: Terminated by Timeout
Monitor duration	188.80s
Return Code	Unknown
PID	1600
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\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0xd10	0x2830000(42139648)	0x5000	✓	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0xd10	0x2840000(42205184)	0x16000	✓	1
Create Remote Thread	#2: c:\users\rdhj0cnfevzx\desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	0xd10	0x2841920(42211616)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih	185.50 KB	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed	✗

Host Behavior

Type	Count
Module	19
System	11077
Process	19848
Mutex	1
Registry	2
File	19
User	1
COM	1

Network Behavior

Type	Count
HTTP	10
TCP	2

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: 194355, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 323864, Reason: Terminated by Timeout
Monitor duration	129.51s
Return Code	Unknown
PID	96
Parent PID	536
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: 204968, Reason: Child Process
Unmonitor End Time	End Time: 323864, Reason: Terminated by Timeout
Monitor duration	118.90s
Return Code	Unknown
PID	604
Parent PID	96
Bitness	32 Bit

Host Behavior

Type	Count
Module	9
File	3
Environment	1
System	574

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed	C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih, C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	Sample File	185.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.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, Create, Delete, Write	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

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://gejajoo7.top	-	-	-	POST	MALICIOUS
http://sysaheu9.top	-	-	-	POST	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
gejajoo7.top	-	-	HTTP	CLEAN
sysaheu9.top	-	-	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	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	CLEAN
\REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI	access	d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	access, read	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.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 (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SmokeLoader	SmokeLoader memory dump	Memory Dump	-	Downloader	5/5

Antivirus (6)

File Type	Threat Name	File Name	Verdict
Sample File	Gen:Variant.Fragtor.35416	C:\Users\RDhJ0CNFevzX\Desktop\d836a03e0b7eeabbc971de7d3e6fcc11bf06e13e633d11118c7429b3abb3c4ed.exe	MALICIOUS
Memory Dump	Generic.Andromeda.D4A614B0	-	MALICIOUS
Memory Dump	Generic.Andromeda.79093CCD	-	MALICIOUS
Memory Dump	Gen:Variant.Razy.655877	-	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 / 10/25/2021 03:57
Static Engine Version	4.3.1.0 / 2021-10-25 03:00:16
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.6 / 2021-09-21 13:25:28
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.18 / 2021-10-22 15:07:52
YARA Built-in Ruleset Version	4.3.1.17

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	2021-10-27 11:33:27+00:00
Built-in AV Database Records	11069139

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