MALICIOUS

Classifications: Injector, Backdoor

Threat Names: AsyncRAT, Gen:Trojan.Heur.IEC.908d4036d15, Gen:Variant.Graftor.946163

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe**
ID	#2782142
MD5	133c10454108aa86301f79a03aa24046
SHA1	21439179cb8700406d57332079ab311d08b0c9bf
SHA256	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797
File Size	650.41 KB
Report Created	2021-09-28 09:39 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 13 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Backdoor
	• Rule "AsyncRAT" from ruleset "RATs" has matched on a memory dump for (process #2) regasm.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected the sample itself as "Gen:Trojan.Heur.IEC.908d4036d15". • Built-in AV detected a memory dump of (process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe as "Gen:Variant.Graftor.946163".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe modifies memory of (process #2) regasm.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe alters context of (process #2) regasm.exe.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\cf\ct.exe" to Windows startup via registry.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe starts (process #2) regasm.exe with a hidden window.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Mutex	Creates mutex	1	-
	• (Process #2) regasm.exe creates mutex with name "df4Rtg34dFjwr".			
1/5	Network Connection	All network connection attempts failed	1	-
	• Host "185.157.160.136" is unavailable.			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) regasm.exe opens an outgoing TCP connection to host "185.157.160.136:1973".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) regasm.exe tries to connect to TCP port 1973 at 185.157.160.136.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe resolves 78 API functions by name.			
-	Trusted	Known clean file	1	-
	• Embedded file "" is a known clean file.			

Mitre ATT&CK Matrix

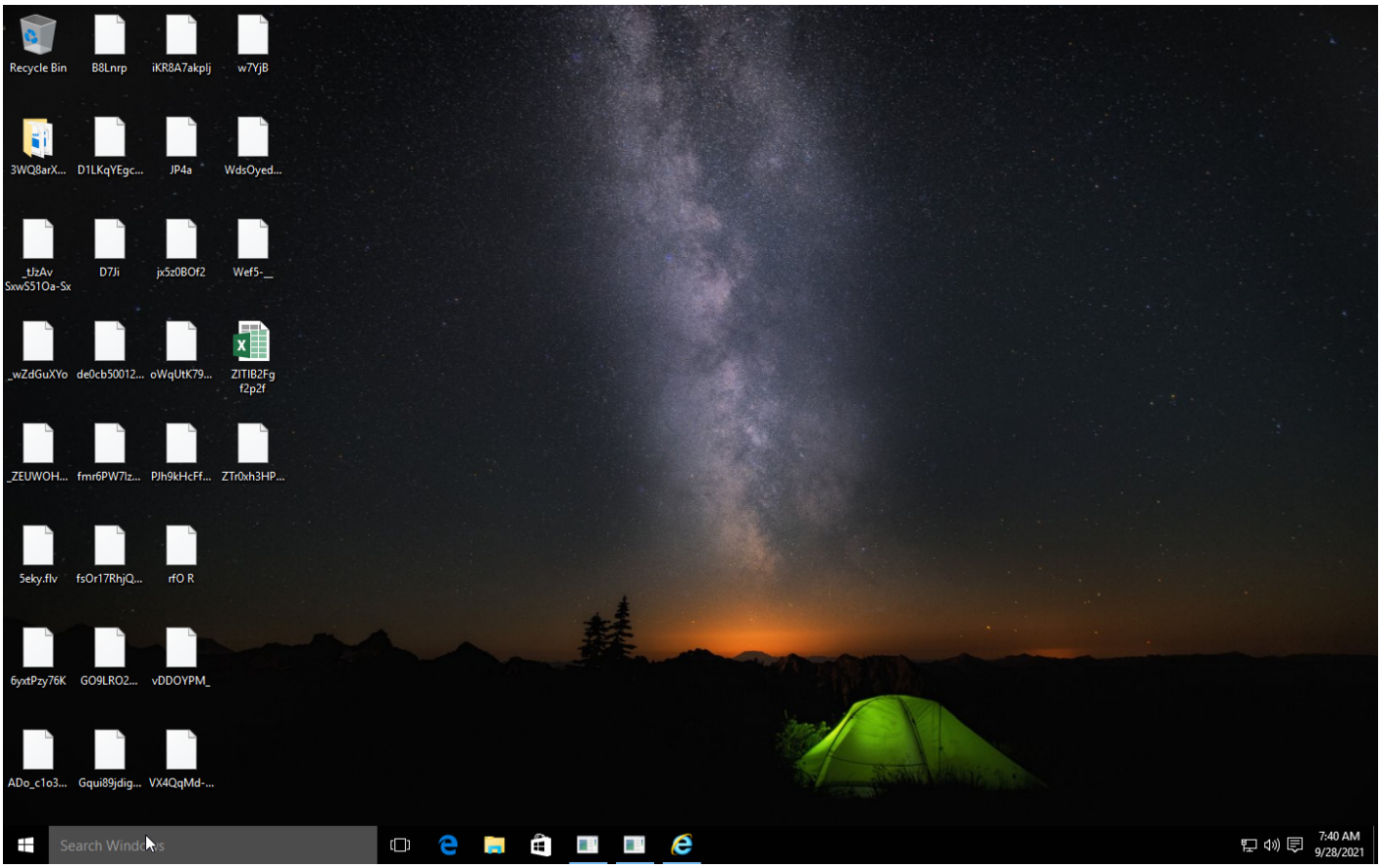
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry					#T1065 Uncommonly Used Port		
				#T1143 Hidden Window							
				#T1045 Software Packing							

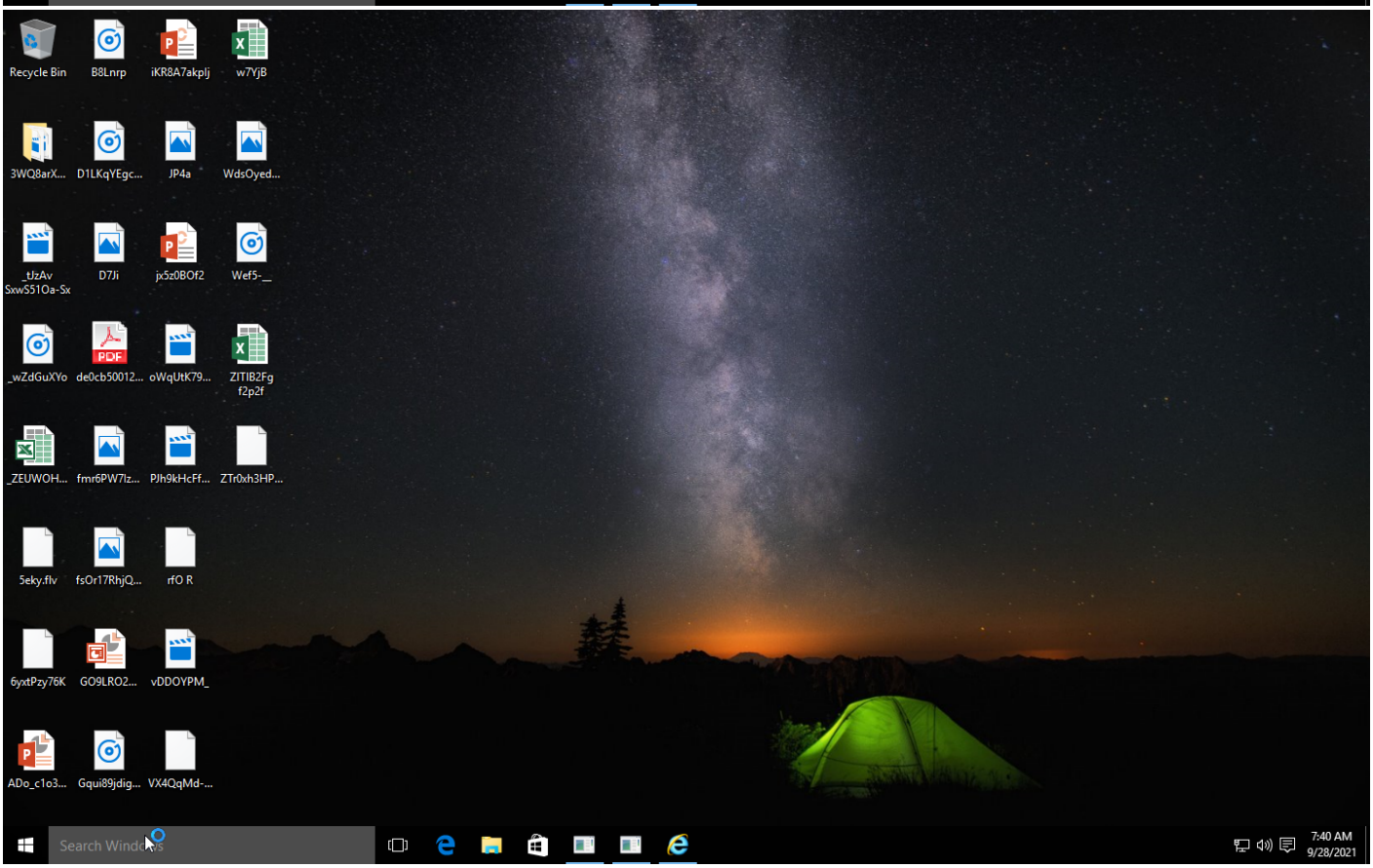
Sample Information

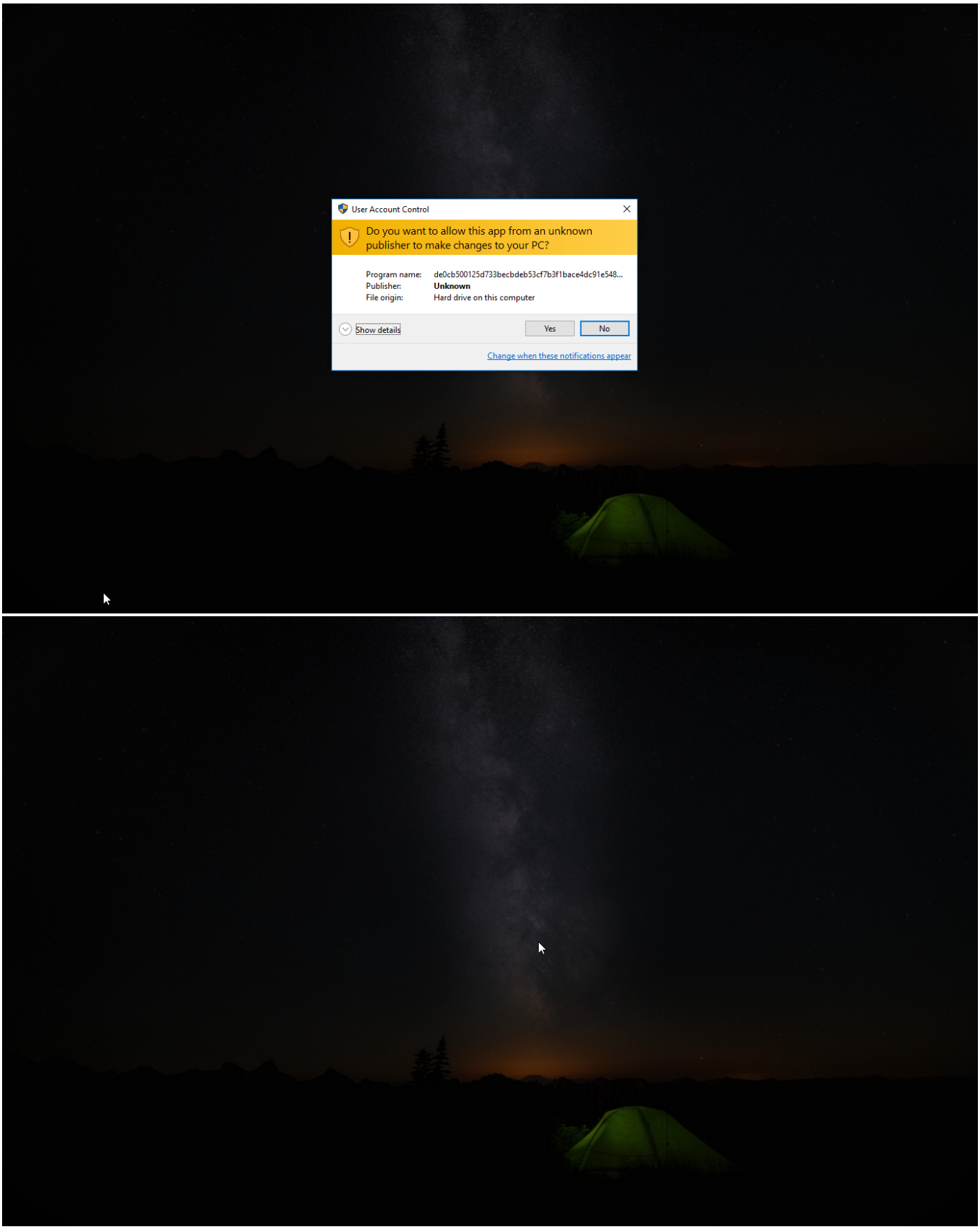
ID	#2782142
MD5	133c10454108aa86301f79a03aa24046
SHA1	21439179cb8700406d57332079ab311d08b0c9bf
SHA256	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797
SSDeep	6144:Xsh7P4K387yYg9ihPBJ1G08ozfjqXXTewGJX/MHeKPwE+8sS6rU8jcxJ8:8h7l38OKJBWkzfwS/M+KGtLHX
ImpHash	835f485ca718411734d873f35af1695e
File Name	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe
File Size	650.41 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 09:39 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
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	4
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	1


Recycle Bin
B8Lnrp
iKR8A7akplj
w7YjB
3WQ8arX...
D1LKqYEgc...
JP4a
WdsOyed...
_tJzAv SxwS51Oa-Sx
D7Ji
jx5z0BOf2
Wef5-_
_wZdGuXYo
de0cb50012...
oWqUtK79...
ZITIB2Fg f2p2f
_ZEUWOH...
fmr6PW7lz...
PJh9kHcFf...
ZTr0xh3HP...
5eky.flv
fsOr17RhjQ...
rfO R
6yxtPzy76K
GO9LRO2...
vDDOYPM_
ADo_c1o3...
Gqui89jdig...
VX4QqMd-...
Search Windows
7:40 AM
9/28/2021


Recycle Bin
B8Lnrp
iKR8A7akplj
w7YjB
3WQ8arX...
D1LKqYEgc...
JP4a
WdsOyed...
_tJzAv SxwS51Oa-Sx
D7Ji
jx5z0BOf2
Wef5-_
_wZdGuXYo
de0cb50012...
oWqUtK79...
ZITIB2Fg f2p2f
_ZEUWOH...
fmr6PW7lz...
PJh9kHcFf...
ZTr0xh3HP...
5eky.flv
fsOr17RhjQ...
rfO R
6yxtPzy76K
GO9LRO2...
vDDOYPM_
ADo_c1o3...
Gqui89jdig...
VX4QqMd-...
Search Windows
7:40 AM
9/28/2021



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 1973

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

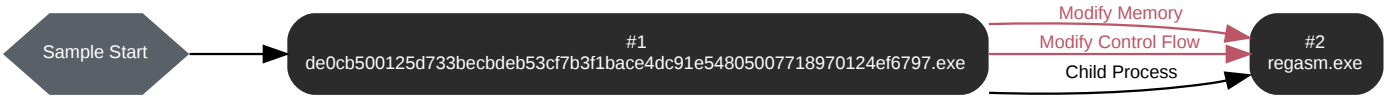
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 59530, Reason: Analysis Target
Unmonitor End Time	End Time: 91536, Reason: Terminated
Monitor duration	32.01s
Return Code	0
PID	2148
Parent PID	1600
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\cf\ct.exe	650.41 KB	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797	✗

Host Behavior

Type	Count
System	11
Module	110
Environment	1
File	48
-	2
Mutex	1
Window	11
Registry	8
Keyboard	1
COM	6
Process	1
-	6
-	3
-	2

Process #2: regasm.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\regasm.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 87282, Reason: Child Process
Unmonitor End Time	End Time: 112601, Reason: Terminated
Monitor duration	25.32s
Return Code	1073807364
PID	880
Parent PID	2148
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	0xa7c	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	0xa7c	0x410000(4259840)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	0xa7c	0x40e000(4251648)	0x800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	0xa7c	0x402000(4202496)	0xa800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	0xa7c	0x287008(2650120)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	0xa7c / 0x4d0	0x77968fe0(2006355936)	-	✓	1

Host Behavior

Type	Count
System	3
User	1
File	25
Mutex	1

Network Behavior

Type	Count
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797	C:\Users\RDhJ0CNFevzX\AppData\Roaming\cf\ct.exe, C:\Users\RDhJ0CNFevzX\Desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	Sample File	650.41 KB	application/vnd.microsoft.portable-executable	Access, Write, Read, Create	MALICIOUS
d9c17df04c721f2aa4bccdca72fb2624d25dda1c22fbf90329f2979e2d21db0b	-	Embedded File	52.50 KB	application/vnd.microsoft.portable-executable	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	Sample File	Access, Read, Create	CLEAN
C:\Windows\SYSTEM32\MSVBVM60.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\cf\ct.exe	Sample File	Access, Write, Create	CLEAN
WINHELP.INI	Accessed File	Access, Read	CLEAN
C:\Windows\SYSTEM32\.HLP	Accessed File	Access	CLEAN
C:\Windows\Help\.HLP	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe.Config	Accessed File	Access, Read	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.157.160.136	-	Sweden	TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
df4Rtg34dFjwr	access	regasm.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors	access	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\cp	access, write	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows	access	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HTML Help	access	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HTML Help\.HLP	access, read	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Help	access	de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	CLEAN

Process

Process Name	Commandline	Verdict
de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	"C:\Users\RDhJ0CNFevzX\Desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e5480500771897012 4ef6797.exe"	MALICIOUS
regasm.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	SUSPICIOUS

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	AsyncRAT	AsyncRAT	Memory Dump	-	Backdoor	5/5

Antivirus (4)

File Type	Threat Name	File Name	Verdict
Sample File	Gen:Trojan.Heur.IEC.908d4036d15	C:\Users\RDhJ0CNFevzX\Desktop\de0cb500125d733becbdeb53cf7b3f1bace4dc91e54805007718970124ef6797.exe	MALICIOUS
Memory Dump	Gen:Variant.Graftor.946163	-	MALICIOUS
Memory Dump	Gen:Variant.Graftor.946163	-	MALICIOUS
Memory Dump	Gen:Variant.Graftor.946163	-	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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

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	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

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