MALICIOUS

Classifications: Downloader

Threat Names: Trojan.Agent.FYJF, Generic.Exploit.Shellcode.RDI.2.2539BF14, Emotet, Gen:Variant.Ulise.385083, Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows ActiveX Control (x86-64)**
File Name	**5Dq6sWcmD.dll.ocx**
ID	#3113497
MD5	b232b0df5d369ef0f7597f215c32043a
SHA1	4a4fb865f1243ea1983044337500448e38557af0
SHA256	19fcf233637e0ca65c4eef3b234d3c79ad1604b524da1b1f292cf7e7dcaf13aa
File Size	548.00 KB
Report Created	2022-10-10 01:21 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 19 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Emotet configuration was extracted	1	Downloader
	• A configuration for Emotet was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	3	Downloader
	• Rule "EmotetEccDecryption" from ruleset "Malware" has matched on a memory dump for (process #2) regsvr32.exe. • Rule "EmotetEccDecryption" from ruleset "Malware" has matched on a memory dump for (process #3) regsvr32.exe. • Rule "EmotetFunctionStrings" from ruleset "Malware" has matched on the function strings for (process #3) regsvr32.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #2) regsvr32.exe tries to delete zone identifier of file "C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll".			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected a memory dump of (Process #2) regsvr32.exe as "Gen:Variant.Ulise.385083". • Built-in AV detected the sample itself as "Trojan.Agent.FYJF". • Built-in AV detected a memory dump of (Process #2) regsvr32.exe as "Generic.Exploit.Shellcode.RDI.2.2539BF14".			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the URL "https://167.172.248.70/" which was contacted by (process #3) regsvr32.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "https://104.168.155.143/" which was contacted by (process #3) regsvr32.exe as Mal/HTMLGen-A.			
4/5	Reputation	Contacts known malicious IP address	2	-
	• Reputation analysis labels the contacted IP address 104.168.155.143 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 167.172.248.70 as Mal/HTMLGen-A.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #6) ipconfig.exe reads the network adapters' addresses by API.			
1/5	Discovery	Enumerates running processes	2	-
	• (Process #2) regsvr32.exe enumerates running processes. • (Process #3) regsvr32.exe enumerates running processes.			
1/5	System Modification	Modifies operating system directory	1	-
	• (Process #2) regsvr32.exe creates file "C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll" in the OS directory.			
1/5	Persistence	Installs system service	1	-
	• (Process #2) regsvr32.exe installs service "GQeyw.dll" via CreateServiceW.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #2) regsvr32.exe starts (process #2) regsvr32.exe with a hidden window. • (Process #3) regsvr32.exe starts (process #3) regsvr32.exe with a hidden window.			

Malware Configuration: Emotet

	Url	https://82.223.21.224:8080
	Url	https://173.212.193.249:8080
	Url	https://82.165.152.127:8080
	Url	https://151.106.112.196:8080
	Url	https://160.16.142.56:8080
	Url	https://163.44.196.120:8080
	Url	https://103.70.28.102:8080
	Url	https://164.68.99.3:8080
	Url	https://51.161.73.194:443
	Url	https://146.59.226.45:443
	Url	https://104.168.155.143:8080
	Url	https://101.50.0.91:8080
	Url	https://94.23.45.86:4143
	Url	https://167.172.253.162:8080
	Url	https://5.9.116.246:8080
	Url	https://185.4.135.165:8080
	Url	https://159.65.140.115:443
	Url	https://212.24.98.99:8080
	Url	https://209.97.163.214:443
	Url	https://206.189.28.199:8080
	Url	https://135.148.6.80:443
	Url	https://159.65.88.10:8080
	Url	https://79.137.35.198:8080
	Url	https://172.105.226.75:8080
	Url	https://172.104.251.154:8080
	Url	https://115.68.227.76:8080
	Url	https://201.94.166.162:443
	Url	https://144.91.78.55:443
	Url	https://183.111.227.137:8080
	Url	https://45.176.232.124:443
	Url	https://209.126.98.206:8080
URL	Url	https://72.15.201.15:8080
	Url	https://197.242.150.244:8080
	Url	https://51.254.140.238:7080
	Url	https://45.235.8.30:8080
	Url	https://103.75.201.2:443
	Url	https://207.148.79.14:8080
	Url	https://213.239.212.5:443
	Url	https://110.232.117.186:8080
	Url	https://153.126.146.25:7080
	Url	https://188.44.20.25:443
	Url	https://134.122.66.193:8080
	Url	https://131.100.24.231:80
	Url	https://186.194.240.217:443
	Url	https://64.227.100.222:8080
	Url	https://51.91.76.89:8080
	Url	https://159.89.202.34:443
	Url	https://149.56.131.28:8080
	Url	https://196.218.30.83:443
	Url	https://103.43.75.120:443
	Url	https://213.241.20.155:443
	Url	https://91.207.28.33:8080
	Url	https://129.232.188.93:443
	Url	https://119.193.124.41:7080
	Url	https://45.118.115.99:8080
	Url	https://158.69.222.101:443
	Url	https://50.35.66.124:8080

Mitre ATT&CK Matrix

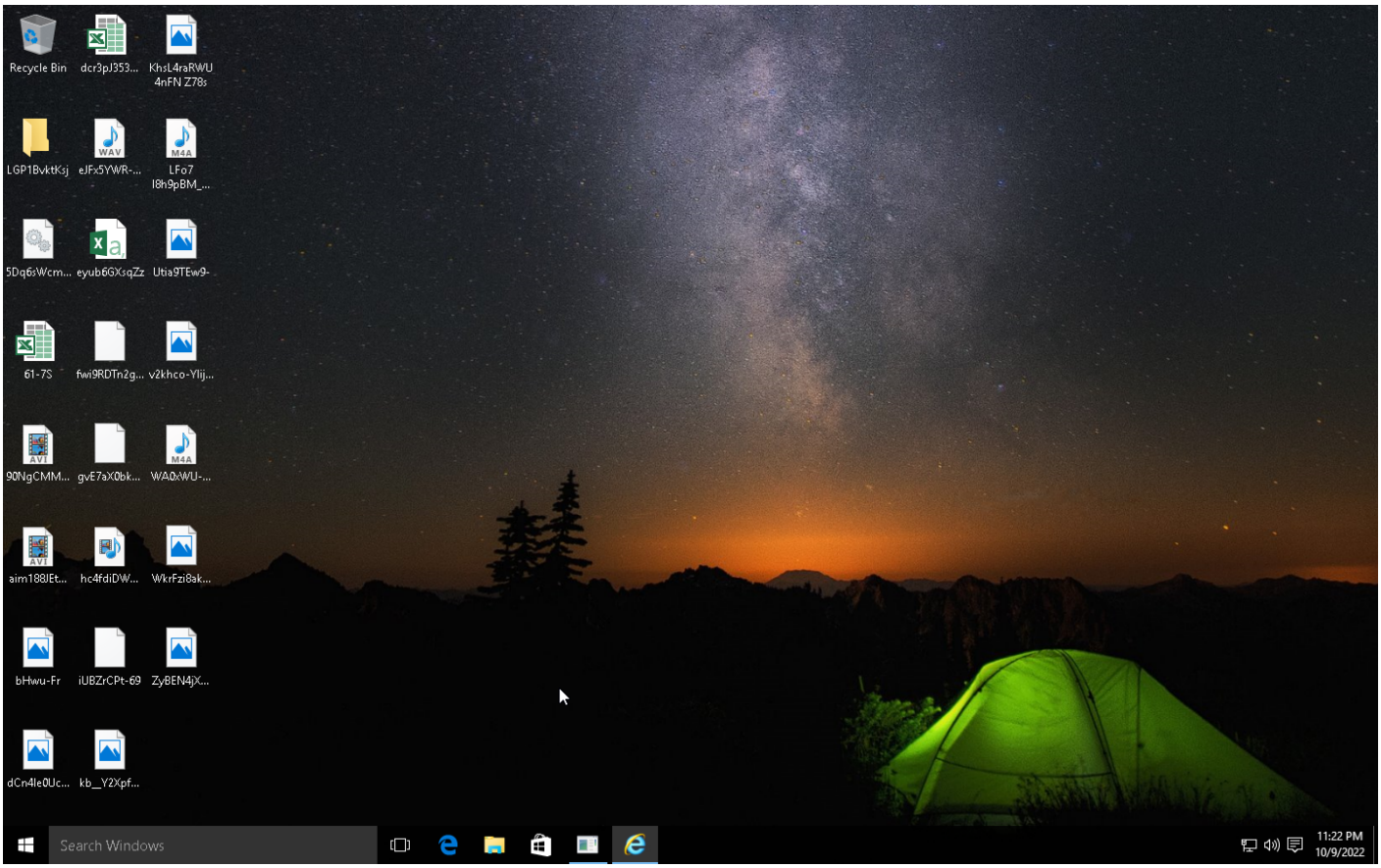
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1050 New Service	#T1050 New Service	#T1096 NTFS File Attributes		#T1057 Process Discovery					
				#T1143 Hidden Window		#T1016 System Network Configuration Discovery					

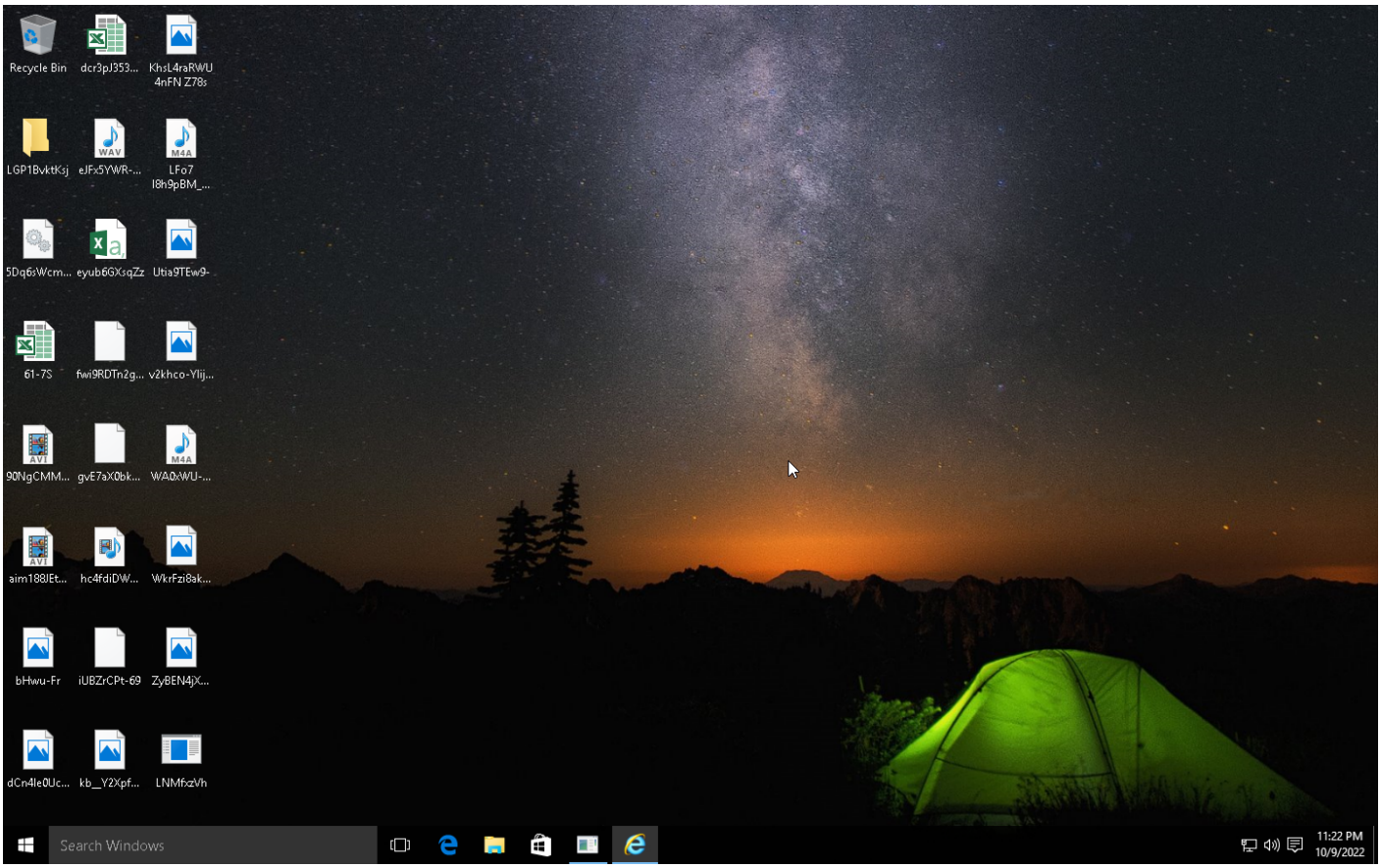
Sample Information

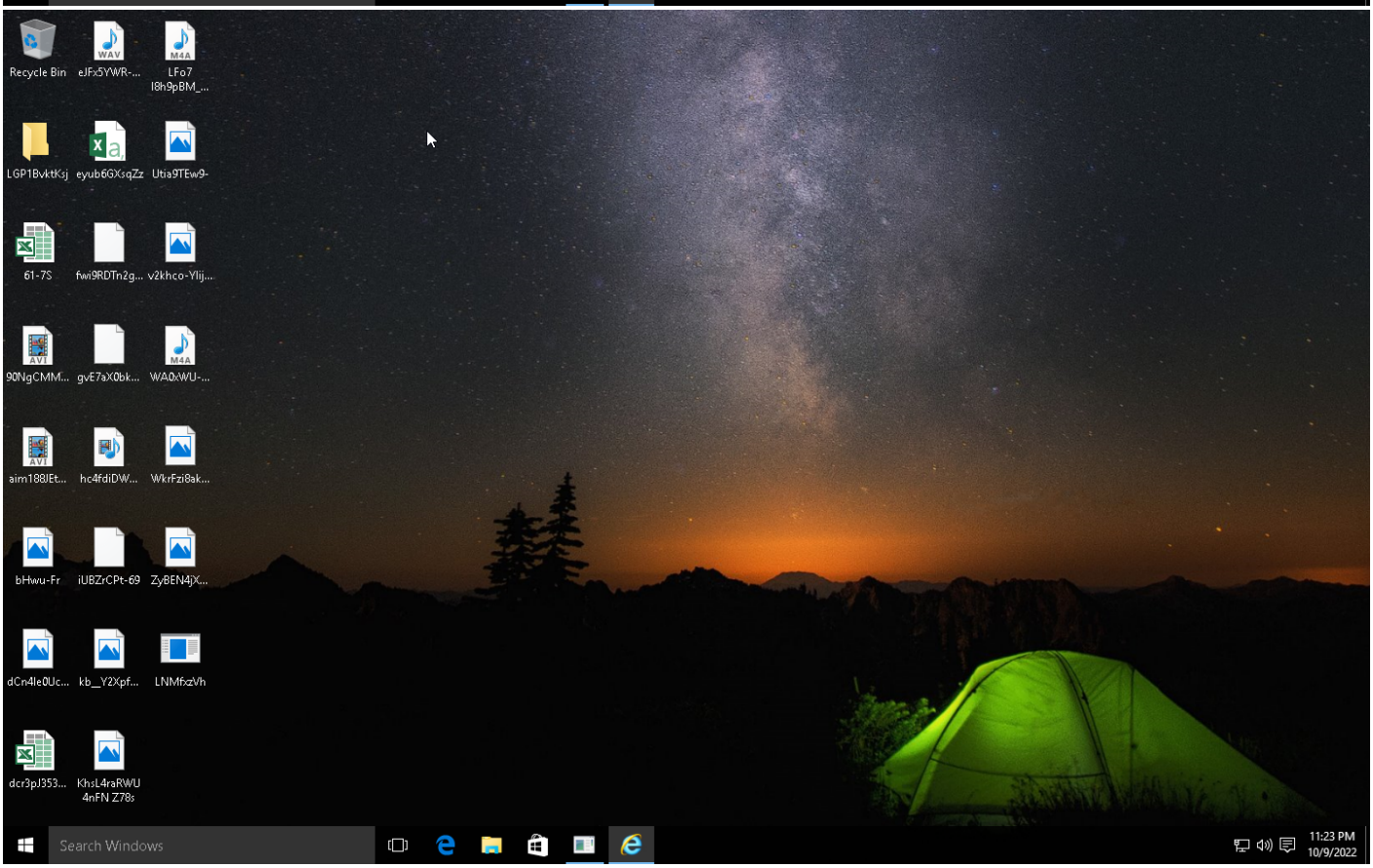
ID	#3113497
MD5	b232b0df5d369ef0f7597f215c32043a
SHA1	4a4fb865f1243ea19830443375004448e38557af0
SHA256	19fcf233637e0ca65c4eef3b234d3c79ad1604b524da1b1f292cf7e7dcaf13aa
SSDeep	12288:Zt5888qi2yYmoYa8Zp3C/EogW4cpaxUhNV/b/:Zz7coTg3C/a3clgJb
ImpHash	089cd79cc1eaac3fa7d34f758db58a4a
File Name	5Dq6sWcmD.dll.ocx
File Size	548.00 KB
Sample Type	Windows ActiveX Control (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2022-10-10 01:21 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
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	4


Recycle Bin
dcr3pJ353...
KhsL4raRWU 4nFN Z78s
LGP1BvktKsj
eJFx5YWR-...
LFo7 I8h9pBM_...
5Dq6sWcm...
eyub6GXsqZz
Utia9TEw9-
61-7S
fwi9RDTn2g...
v2khco-Ylij...
90NgCMM...
gvE7aX0bk...
WAQxWU-...
aim188lEt...
hc4fdiDW...
WkrFzi8ak...
bHwu-Fr
iUBZrCPt-69
ZyBEN4jX...
dCn4le0Uc...
kb_Y2Xpf...
Search Windows
11:22 PM
10/9/2022





Screenshots truncated

NETWORK

General

9.26 KB total sent

139.69 KB total received

1 ports 8080

2 contacted IP addresses

64 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

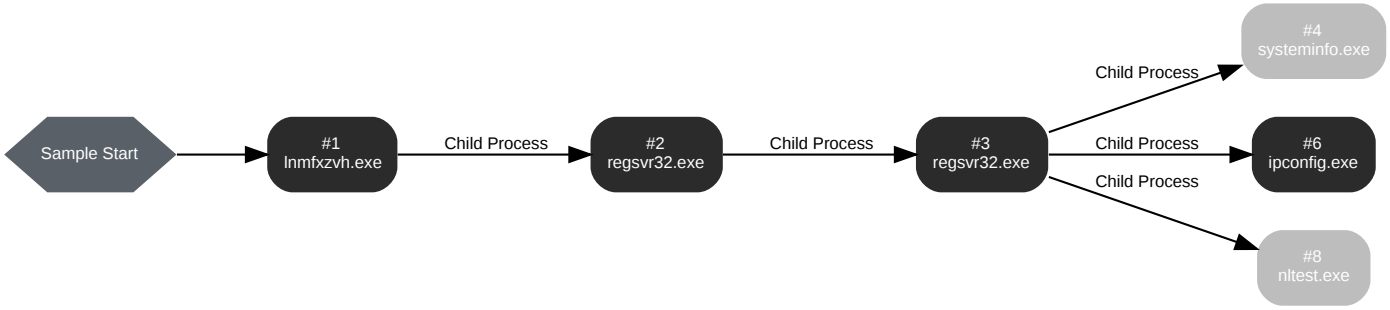
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: lnmfxzvh.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\lnmfxzvh.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\LNMfxzVh.exe" "C:\Users\RDHJ0C~1\Desktop\5Dq6sWcmD.dll.ocx"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 59883, Reason: Analysis Target
Unmonitor End Time	End Time: 96119, Reason: Terminated
Monitor duration	36.24s
Return Code	0
PID	3300
Parent PID	2044
Bitness	64 Bit

Host Behavior

Type	Count
Module	19
File	3
Environment	1
Registry	4
Process	1

Process #2: regsvr32.exe

ID	2
File Name	c:\windows\system32\regsvr32.exe
Command Line	"C:\Windows\System32\regsvr32.exe" "C:\Users\RDHJ0C~1\Desktop\5Dq6sWcmD.dll.ocx"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81685, Reason: Child Process
Unmonitor End Time	End Time: 95417, Reason: Terminated
Monitor duration	13.73s
Return Code	0
PID	2900
Parent PID	3300
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\5Dq6sWcmD.dll.ocx	548.00 KB	19fcf233637e0ca65c4eef3b234d3c79ad1604b524da1b1f292cf7e7dcaf13aa	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	42
Registry	4
File	5
Environment	1
System	2
-	7
Process	111

Process #3: regsvr32.exe

ID	3
File Name	c:\windows\system32\regsvr32.exe
Command Line	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94325, Reason: Child Process
Unmonitor End Time	End Time: 129387, Reason: Terminated
Monitor duration	35.06s
Return Code	1073807364
PID	3552
Parent PID	2900
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\E6FE.tmp	2.28 KB	dc8d4e5a70e7afc4b5795af73cabd4f4628077ca739be04da4618341d2b61532	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\D1EE.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\EBF0.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	37
Registry	4
System	6
-	1
Process	326
-	2
File	16
Keyboard	3

Process #4: systeminfo.exe

ID	4
File Name	c:\windows\system32\systeminfo.exe
Command Line	systeminfo
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117624, Reason: Child Process
Unmonitor End Time	End Time: 122933, Reason: Terminated
Monitor duration	5.31s
Return Code	1073807364
PID	4520
Parent PID	3552
Bitness	64 Bit

Process #6: ipconfig.exe

ID	6
File Name	c:\windows\system32\ipconfig.exe
Command Line	ipconfig /all
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 122929, Reason: Child Process
Unmonitor End Time	End Time: 125241, Reason: Terminated
Monitor duration	2.31s
Return Code	0
PID	3172
Parent PID	3552
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	128
Environment	43
System	6
Registry	7

Process #8: nltest.exe

ID	8
File Name	c:\windows\system32\nltest.exe
Command Line	nltest /dclist:
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 124197, Reason: Child Process
Unmonitor End Time	End Time: 126400, Reason: Terminated
Monitor duration	2.20s
Return Code	0
PID	3376
Parent PID	3552
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
19fcf233637e0ca65c4eef3b234d3c79ad1604b524da1b1f292cf7e7dcaf13aa	C:\Users\RDhJ0CNFevzX\Desktop\5Dq6sWcmD.dll.ocx, C:\Users\RDHJ0C~1\Desktop\5Dq6sWcmD.dll.ocx, C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll	Sample File	548.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
dc8d4e5a70e7afc4b5795af73cabd4f4628077ca739be04da4618341d2b61532	C:\Users\RDHJ0C~1\AppData\Local\Temp\E6FE.tmp	Dropped File	2.28 KB	text/plain	Access, Create, Delete, Read	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\5Dq6sWcmD.dll.ocx	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDHJ0C~1\AppData\Local\Temp\D1EE.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\5Dq6sWcmD.dll.ocx	Accessed File	Access, Delete	CLEAN
-	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\E6FE.tmp	Dropped File, Accessed File	Access, Create, Delete, Read	CLEAN
C:\Windows\System32\regsvr32.exe	Accessed File	Access	CLEAN
c:\srvsvc	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\LNMfxzVh.exe	Accessed File	Access	CLEAN
C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll	-	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\EBF0.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete, Read	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://188.44.20.25	-	188.44.20.25	-	-	MALICIOUS
https://107.170.39.149:8080	-	107.170.39.149	-	-	MALICIOUS
https://206.189.28.199:8080	-	206.189.28.199	-	-	MALICIOUS
https://45.235.8.30:8080	-	45.235.8.30	-	-	MALICIOUS
https://183.111.227.137:8080	-	183.111.227.137	-	-	MALICIOUS
https://163.44.196.120:8080	-	163.44.196.120	-	-	MALICIOUS
https://159.89.202.34	-	159.89.202.34	-	-	MALICIOUS
https://197.242.150.244:8080	-	197.242.150.244	-	-	MALICIOUS
https://201.94.166.162	-	201.94.166.162	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://103.75.201.2	-	103.75.201.2	-	-	MALICIOUS
https://146.59.226.45	-	146.59.226.45	-	-	MALICIOUS
https://151.106.112.196:8080	-	151.106.112.196	-	-	MALICIOUS
https://153.126.146.25:7080	-	153.126.146.25	-	-	MALICIOUS
https://160.16.142.56:8080	-	160.16.142.56	-	-	MALICIOUS
https://110.232.117.186:8080	-	110.232.117.186	-	-	MALICIOUS
https://103.43.75.120	-	103.43.75.120	-	-	MALICIOUS
https://119.193.124.41:7080	-	119.193.124.41	-	-	MALICIOUS
http://0.0.0.0	-	0.0.0.0	-	-	MALICIOUS
https://79.137.35.198:8080	-	79.137.35.198	-	-	MALICIOUS
https://207.148.79.14:8080	-	207.148.79.14	-	-	MALICIOUS
https://103.132.242.26:8080	-	103.132.242.26	-	-	MALICIOUS
https://139.59.126.41	-	139.59.126.41	-	-	MALICIOUS
https://196.218.30.83	-	196.218.30.83	-	-	MALICIOUS
https://159.65.88.10:8080	-	159.65.88.10	-	-	MALICIOUS
https://135.148.6.80	-	135.148.6.80	-	-	MALICIOUS
https://212.24.98.99:8080	-	212.24.98.99	-	-	MALICIOUS
https://134.122.66.193:8080	-	134.122.66.193	-	-	MALICIOUS
https://172.104.251.154:8080	-	172.104.251.154	-	-	MALICIOUS
https://115.68.227.76:8080	-	115.68.227.76	-	-	MALICIOUS
https://144.91.78.55	-	144.91.78.55	-	-	MALICIOUS
https://101.50.0.91:8080	-	101.50.0.91	-	-	MALICIOUS
https://64.227.100.222:8080	-	64.227.100.222	-	-	MALICIOUS
https://51.161.73.194	-	51.161.73.194	-	-	MALICIOUS
https://91.207.28.33:8080	-	91.207.28.33	-	-	MALICIOUS
https://103.70.28.102:8080	-	103.70.28.102	-	-	MALICIOUS
https://185.4.135.165:8080	-	185.4.135.165	-	-	MALICIOUS
https://51.254.140.238:7080	-	51.254.140.238	-	-	MALICIOUS
https://1.234.2.232:8080	-	1.234.2.232	-	-	MALICIOUS
https://167.172.248.70	-	167.172.248.70	-	-	MALICIOUS
https://150.95.66.124:8080	-	150.95.66.124	-	-	MALICIOUS
https://167.172.253.162:8080	-	167.172.253.162	-	-	MALICIOUS
https://5.9.116.246:8080	-	5.9.116.246	-	-	MALICIOUS
https://172.105.226.75:8080	-	172.105.226.75	-	-	MALICIOUS
https://94.23.45.86:4143	-	94.23.45.86	-	-	MALICIOUS
https://45.176.232.124	-	45.176.232.124	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://45.118.115.99:8080	-	45.118.115.99	-	-	MALICIOUS
https://158.69.222.101	-	158.69.222.101	-	-	MALICIOUS
https://164.68.99.3:8080	-	164.68.99.3	-	-	MALICIOUS
https://186.194.240.217	-	186.194.240.217	-	-	MALICIOUS
https://149.56.131.28:8080	-	149.56.131.28	-	-	MALICIOUS
https://213.241.20.155	-	213.241.20.155	-	-	MALICIOUS
https://72.15.201.15:8080	-	72.15.201.15	-	-	MALICIOUS
https://209.97.163.214	-	209.97.163.214	-	-	MALICIOUS
https://131.100.24.231:80	-	131.100.24.231	-	-	MALICIOUS
https://209.126.98.206:8080	-	209.126.98.206	-	-	MALICIOUS
https://104.168.155.143:8080	-	104.168.155.143	-	-	MALICIOUS
https://82.165.152.127:8080	-	82.165.152.127	-	-	MALICIOUS
https://82.223.21.224:8080	-	82.223.21.224	-	-	MALICIOUS
https://213.239.212.5	-	213.239.212.5	-	-	MALICIOUS
https://51.91.76.89:8080	-	51.91.76.89	-	-	MALICIOUS
https://129.232.188.93	-	129.232.188.93	-	-	MALICIOUS
https://104.168.155.143	-	104.168.155.143	-	-	MALICIOUS
https://173.212.193.249:8080	-	173.212.193.249	-	-	MALICIOUS
https://159.65.140.115	-	159.65.140.115	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
167.172.248.70	-	United States	TCP, TLS	MALICIOUS
104.168.155.143	-	United States	TCP, TLS	MALICIOUS
173.212.193.249	-	-	-	CLEAN
172.105.226.75	-	-	-	CLEAN
1.234.2.232	-	-	-	CLEAN
150.95.66.124	-	-	-	CLEAN
101.50.0.91	-	-	-	CLEAN
51.254.140.238	-	-	-	CLEAN
186.194.240.217	-	-	-	CLEAN
134.122.66.193	-	-	-	CLEAN
94.23.45.86	-	-	-	CLEAN
103.43.75.120	-	-	-	CLEAN
129.232.188.93	-	-	-	CLEAN
64.227.100.222	-	-	-	CLEAN
146.59.226.45	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
139.59.126.41	-	-	-	CLEAN
151.106.112.196	-	-	-	CLEAN
201.94.166.162	-	-	-	CLEAN
51.161.73.194	-	-	-	CLEAN
163.44.196.120	-	-	-	CLEAN
209.97.163.214	-	-	-	CLEAN
45.235.8.30	-	-	-	CLEAN
115.68.227.76	-	-	-	CLEAN
107.170.39.149	-	-	-	CLEAN
164.68.99.3	-	-	-	CLEAN
5.9.116.246	-	-	-	CLEAN
144.91.78.55	-	-	-	CLEAN
103.75.201.2	-	-	-	CLEAN
82.223.21.224	-	-	-	CLEAN
158.69.222.101	-	-	-	CLEAN
207.148.79.14	-	-	-	CLEAN
212.24.98.99	-	-	-	CLEAN
213.241.20.155	-	-	-	CLEAN
149.56.131.28	-	-	-	CLEAN
45.176.232.124	-	-	-	CLEAN
153.126.146.25	-	-	-	CLEAN
51.91.76.89	-	-	-	CLEAN
167.172.253.162	-	-	-	CLEAN
196.218.30.83	-	-	-	CLEAN
159.89.202.34	-	-	-	CLEAN
45.118.115.99	-	-	-	CLEAN
103.132.242.26	-	-	-	CLEAN
79.137.35.198	-	-	-	CLEAN
159.65.140.115	-	-	-	CLEAN
135.148.6.80	-	-	-	CLEAN
206.189.28.199	-	-	-	CLEAN
183.111.227.137	-	-	-	CLEAN
91.207.28.33	-	-	-	CLEAN
110.232.117.186	-	-	-	CLEAN
172.104.251.154	-	-	-	CLEAN
197.242.150.244	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
185.4.135.165	-	-	-	CLEAN
188.44.20.25	-	-	-	CLEAN
131.100.24.231	-	-	-	CLEAN
0.0.0.0	-	-	-	CLEAN
160.16.142.56	-	-	-	CLEAN
209.126.98.206	-	-	-	CLEAN
72.15.201.15	-	-	-	CLEAN
119.193.124.41	-	-	-	CLEAN
82.165.152.127	-	-	-	CLEAN
103.70.28.102	-	-	-	CLEAN
213.239.212.5	-	-	-	CLEAN
159.65.88.10	-	-	-	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}\Dhcpv6ClassId	access, read	ipconfig.exe	CLEAN
HKEY_CLASSES_ROOT\.dll	access, read	regsvr32.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	access	lnmfxzvh.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile\AutoRegister	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\ocxfile	access	regsvr32.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}\Dhcpv6ClassId	access, read	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	access	ipconfig.exe	CLEAN
HKEY_CLASSES_ROOT\.ocx	access, read	regsvr32.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E96D977E-F067-4CE9-924D-F6E0A04729E4}\DhcpClassId	access, read	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	access	ipconfig.exe	CLEAN
HKEY_CLASSES_ROOT\ocxfile\AutoRegister	access	regsvr32.exe	CLEAN

Process

Process Name	Commandline	Verdict
regsvr32.exe	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GnynPsiyLKdYjn\GQeyw.dll"	SUSPICIOUS

Process Name	Commandline	Verdict
ipconfig.exe	ipconfig /all	SUSPICIOUS
regsvr32.exe	"C:\Windows\System32\regsvr32.exe" "C:\Users\RDHJ0C~1\Desktop\5Dq6sWcmD.dll.ocx"	SUSPICIOUS
systeminfo.exe	systeminfo	CLEAN
nltest.exe	nltest /dclist:	CLEAN
lnmfxzvh.exe	"C:\Users\RDhJ0CNFevzX\Desktop\LNMfxzVh.exe" "C:\Users\RDHJ0C~1\Desktop\5Dq6sWcmD.dll.ocx"	CLEAN

YARA / AV

YARA (4)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Malware	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Malware	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Malware	EmotetFunctionStrings	Emotet function strings	Function Strings	-	Downloader	5/5

Antivirus (3)

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Variant.Ulise.385083	-	MALICIOUS
Sample File	Trojan.Agent.FYJF	C:\Users\RDhJ0CNFevzX\Desktop\5Dq6sWcmD.dll.ocx	MALICIOUS
Memory Dump	Generic.Exploit.Shellcode.RDI.2.2539BF14	-	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	4.6.0
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	4.6.2.24 / 2022-09-07 15:06:41
Link Detonation Heuristics Version	4.6.2.24 / 2022-09-07 15:06:41
Smart Memory Dumping Rules Version	4.6.2.24 / 2022-09-07 15:06:41
Config Extractors Version	4.6.2.29 / 2022-09-29 14:02:13
Signature Trust Store Version	4.6.2.24 / 2022-09-07 15:06:41
VMRay Threat Identifiers Version	4.6.2.29 / 2022-09-29 14:02:13
YARA Built-in Ruleset Version	4.6.2.29

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	2022-10-09 17:33:24
Built-in AV Database Records	10012728

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	8.0.1710.11

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