JoeSandbox Cloud BASIC

ID: 433079
Sample Name: dNeoJAgJU5
Cookbook: default.jbs
Time: 09:00:57
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

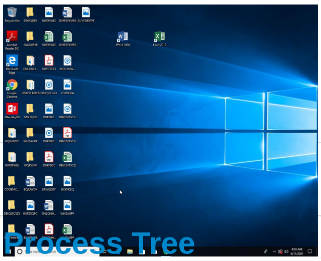
Analysis Report dNeoJAgJU5

Overview

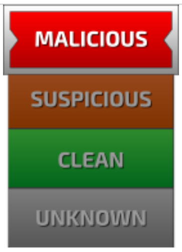
General Information

Sample Name:	dNeoJAgJU5 (renamed file extension from none to exe)
Analysis ID:	433079
MD5:	d2a8ef4a18e3c6d.
SHA1:	7c6bcb0d6e1528..
SHA256:	931959c2c56185..
Tags:	exe trojan
Infos:	

Most interesting Screenshot:



Detection



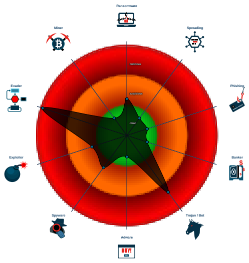
FormBook

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- dNeoJAgJU5.exe (PID: 7144 cmdline: 'C:\Users\user\Desktop\dNeoJAgJU5.exe' MD5: D2A8EF4A18E3C6DC377DAF765B37A9CA)
  - dNeoJAgJU5.exe (PID: 4904 cmdline: C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe MD5: D2A8EF4A18E3C6DC377DAF765B37A9CA)
  - dNeoJAgJU5.exe (PID: 6880 cmdline: C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe MD5: D2A8EF4A18E3C6DC377DAF765B37A9CA)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 5724 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 660 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bucksnortneola.com/gw2/"
  ],
  "decoy": [
    "kmampc.com",
    "swagsoldier.com",
    "achochapo.com",
    "nestymentemaestra.com",
    "rakuen-beans.info",
    "portaldainsolvencia.com",
    "nationaltodaytv.com",
    "monadiclab.com",
    "thebudgetfurnituredenver.com",
    "sifangzhouzi.com",
    "quangcaosonthach.com",
    "cbluebeltliveshop.com",
    "hyperrealmarketing.com",
    "dallasproducecompany.com",
    "zizhizhengshu.com",
    "becosyshe.com",
    "injectionhub.com",
    "wasteshelter.com",
    "gapegod.com",
    "danfrem.com",
    "emag.enterprises",
    "insomniaut.com",
    "margaretsboutiquenb.com",
    "bestmovies4k.com",
    "hsxytz.com",
    "veles.asia",
    "graphicoustic.com",
    "rzeroxi.com",
    "cristyleebennett.com",
    "vercoicsporno.club",
    "awdworldwide.com",
    "agrilast.com",
    "vineyardplaceseniorliving.com",
    "blancaholidaylets.com",
    "didixun.com",
    "localmiller.com",
    "gravityphysiotherapy.com",
    "couchtabledesktop.com",
    "cypresswoodsseniorliving.com",
    "mmdastro.com",
    "opportunitybsi.com",
    "deejspeaks.com",
    "alllivesmattertojesus.info",
    "clippingpathmask.com",
    "tuoitrechuatraisudoi.site",
    "mipecheritage.info",
    "acadeopolis.com",
    "52jnh.com",
    "thetrust.place",
    "highseachartersct.com",
    "booklarge.com",
    "kela-de.com",
    "ea-it-pantomath.com",
    "tricountyrr.com",
    "blackeye.online",
    "hidrovaco.com",
    "sleeplessreconnaissance.life",
    "newalbanyironworks.com",
    "scthxb.com",
    "bossssss.com",
    "isaostar.com",
    "pointredeem.com",
    "myfulfillmentproject.com",
    "toikawai.com"
  ]
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
dNeoJAgJU5.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.801702027.00000000036B5000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.801702027.00000000036B5000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9e88:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa102:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15c25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15711:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15d27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15e9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xab1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1498c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb813:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b8c7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c8ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.801702027.00000000036B5000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x189a9:$sqlite3step: 68 34 1C 7B E1 • 0x18abc:$sqlite3step: 68 34 1C 7B E1 • 0x189d8:$sqlite3text: 68 38 2A 90 C5 • 0x18afd:$sqlite3text: 68 38 2A 90 C5 • 0x189eb:$sqlite3blob: 68 53 D8 7F 8C • 0x18b13:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.796802403.0000000000052000.00000002.00020000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000011.00000002.909870472.0000000000EA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.msdt.exe.556f834.4.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
13.0.dNeoJAgJU5.exe.370000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
13.2.dNeoJAgJU5.exe.370000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
17.2.msdt.exe.556f834.4.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
14.0.dNeoJAgJU5.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 19 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Yara detected Costura Assembly Loader

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

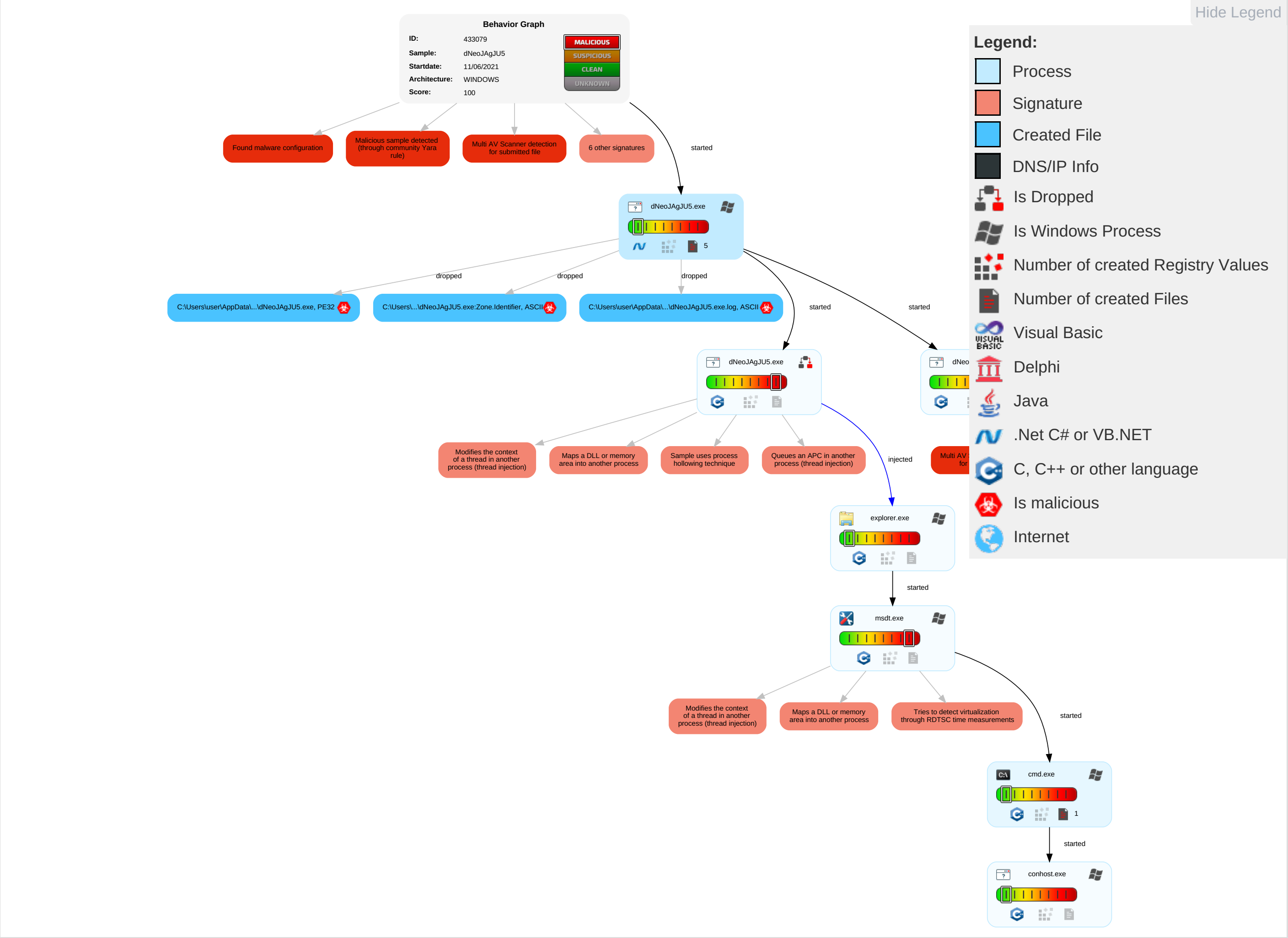
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 4 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communicat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Steganography	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	System Information Discovery 1 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 4 1 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

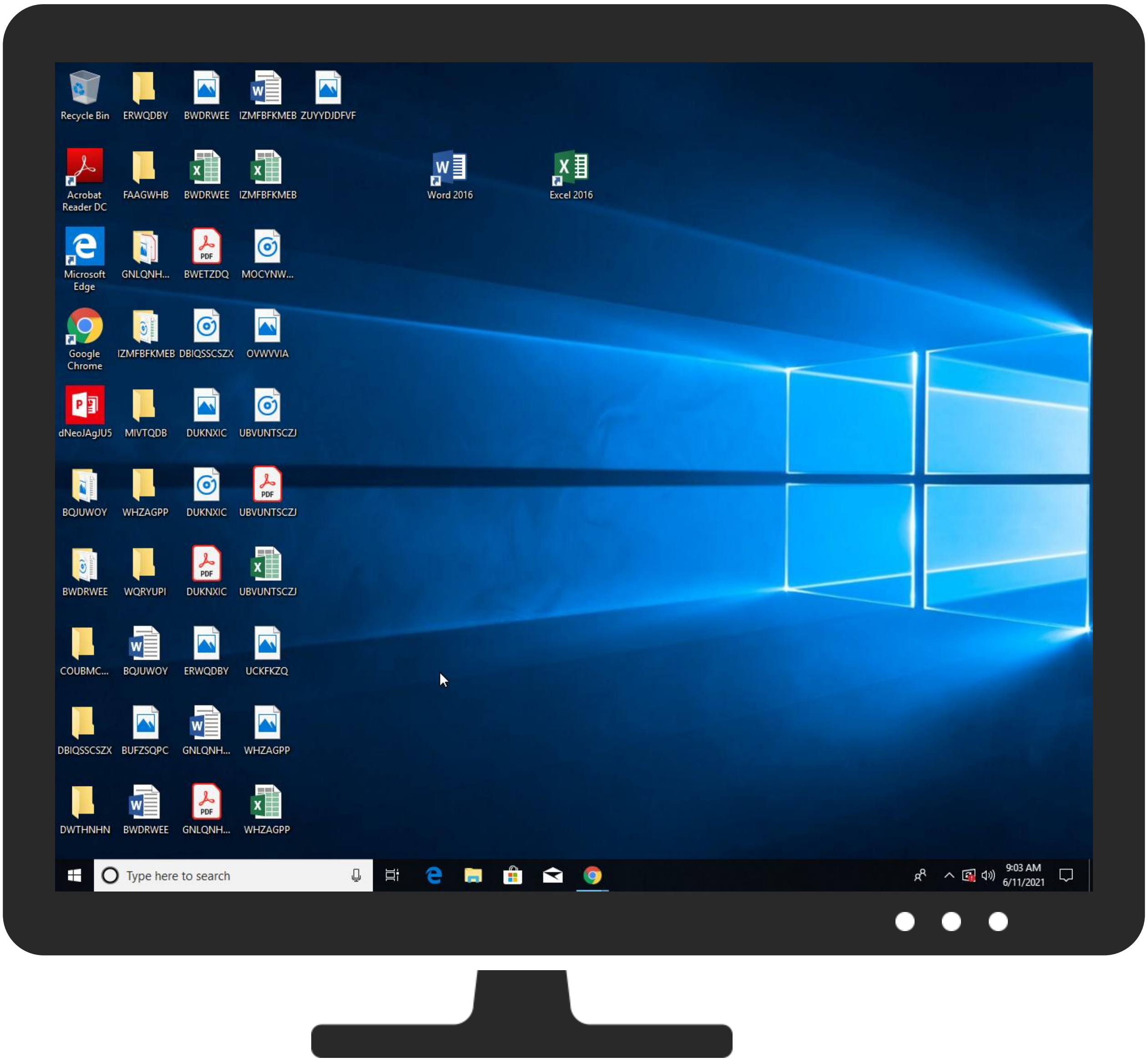
Behavior Graph


Hide Legend
Behavior Graph
ID: 433079
Sample: dNeoJAgJU5
Startdate: 11/06/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Multi AV Scanner detection for submitted file
6 other signatures
started
dNeoJAgJU5.exe
5
dropped
dropped
dropped
C:\Users\user\AppData\...\dNeoJAgJU5.exe, PE32
C:\Users\...\dNeoJAgJU5.exe:Zone.Identifier, ASCII
C:\Users\user\AppData\...\dNeoJAgJU5.exe.log, ASCII
started
started
dNeoJAgJU5.exe
dNeo
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
injected
Multi AV for
explorer.exe
started
msdt.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
cmd.exe
C:\
1
started
conhost.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dNeoJAgJU5.exe	50%	Virustotal		Browse
dNeoJAgJU5.exe	31%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
dNeoJAgJU5.exe	59%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe	59%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.dNeoJAgJU5.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.2.dNeoJAgJU5.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0U	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0U	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0U	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0U	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
www.bucksnortneola.com/gw2/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.bucksnortneola.com/gw2/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433079
Start date:	11.06.2021
Start time:	09:00:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dNeoJAgJU5 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/3@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 16.9%) • Quality average: 75.3% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dNeoJAgJU5.exe.log

Process:	C:\Users\user\Desktop\dNeoJAgJU5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe

Process:	C:\Users\user\Desktop\dNeoJAgJU5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	542192
Entropy (8bit):	7.9453925891427115
Encrypted:	false
SSDEEP:	12288:mQ985Wz2+Q38+VAYy2qoTGWA6Tp2x4tWKG1Gu7iTQezjBw5U1:c5MQ38tpsA6c4tc1Gu7Kzum1
MD5:	D2A8EF4A18E3C6DC377DAF765B37A9CA
SHA1:	7C6BCB0D6E1528AF56B888657A26C186C818493B
SHA-256:	931959C2C56185581AB2639948E3E207C5CB3C1E1C0225567C31F03A5B39E65D
SHA-512:	DBB8C8430A7683632E1AC16CB8BE7F6C4FF0CA37652721E73770E9BB7397C52DA98BE49FC418FBF6DCB6040190FCF05542CF4E210BF33D91629FC0DC09F1AF 7
Malicious:	**true**
Yara Hits:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe, Author: Joe Security
Antivirus:	- Antivirus: Metadefender, Detection: 31%, Browse - Antivirus: ReversingLabs, Detection: 59%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....8.`.....................J......^.... ........@.. ..................................@....................................K........F..............'...`... ....H...........text...d.... ....`.rsrc....F.......H..................@..@.reloc.......`......................@..B................@.......H........7..t-..........$e..:.....:....8....(....8....(....8....*..*...0..........s.....:d...&s.....:b...&s.....:`...&s.........~....r...pr...po....~....rS..prc..po....~....r...pr...po....8.........8.........8.........8....*......:....&:....8....&8....r...p*...:....&o....8....&8....*...0..........(....o.....:....&..:....&8f....8.....8........:$...&.o......o.....o.....(....9....8.....8.....o....(.....o....(.....(....9.....*..X....i

C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\dNeoJAgJU5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe:Zone.Identifier	
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9453925891427115
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	dNeoJAgJU5.exe
File size:	542192
MD5:	d2a8ef4a18e3c6dc377daf765b37a9ca
SHA1:	7c6bcb0d6e1528af56b888657a26c186c818493b
SHA256:	931959c2c56185581ab2639948e3e207c5cb3c1e1c0225567c31f03a5b39e65d
SHA512:	dbb8c8430a7683632e1ac16cb8be7f6c4ff0ca37652721e73770e9bb7397c52da98be49fc418fbf6dcb6040190fcf05542cf4e210bf33d91629fc0dc09f1aff7
SSDEEP:	12288:mQ985Wz2+Q38+VAYy2qoTGWA6Tp2x4tWKG1Gu7iTQezjBw5U1:c5MQ38tpsA6c4tc1Gu7Kzum1
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....8.`.....................J......^.... ....@.. ....@................................

File Icon

Icon Hash:	23d8dcd6d8d81047

Static PE Info

General

Entrypoint:	0x47f15e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C138FF [Wed Jun 9 21:56:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	CN=COMODO RSA Extended Validation Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/7/2019 2:00:00 AM 10/7/2022 1:59:59 AM
Subject Chain	• CN=Telegram FZ-LLC, O=Telegram FZ-LLC, STREET="Business Central Towers, Tower A, Office 2301 2303", L=Dubai, S=Dubai, C=AE, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=AE, SERIALNUMBER=94349
Version:	3
Thumbprint MD5:	034F2391B5CE85A7D99BC43FE240F70F
Thumbprint SHA-1:	D4C89B25D3E92D05B44BC32C0CBFD7693613F3EE
Thumbprint SHA-256:	E31F1B9C3DDD0EDEFDF96F85B8FFD1DB976573BB262CC6E1154AD8FDC4D55449
Serial:	1F3216F428F850BE2C66CAA056F6D821

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7d164	0x7d200	False	0.984230613137	data	7.99020457416	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x46b4	0x4800	False	0.0655924479167	data	2.51724314741	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: dNeoJAgJU5.exe PID: 7144 Parent PID: 6020

General

Start time:	09:01:43
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\dNeoJAgJU5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dNeoJAgJU5.exe'
Imagebase:	0x50000
File size:	542192 bytes
MD5 hash:	D2A8EF4A18E3C6DC377DAF765B37A9CA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.801702027.00000000036B5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.801702027.00000000036B5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.801702027.00000000036B5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000002.796802403.0000000000052000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.800519998.0000000003546000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.800519998.0000000003546000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.800519998.0000000003546000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000000.641852004.0000000000052000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000002.798914394.00000000023F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.801275490.000000000361B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.801275490.000000000361B000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.801275490.000000000361B000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dNeoJAgJU5.exe PID: 4904 Parent PID: 7144

General

Start time:	09:02:54
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe
Imagebase:	0x370000
File size:	542192 bytes
MD5 hash:	D2A8EF4A18E3C6DC377DAF765B37A9CA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.794448799.0000000000372000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000000.793684008.0000000000372000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe, Author: Joe Security
Antivirus matches:	• Detection: 31%, Metadefender, Browse • Detection: 59%, ReversingLabs
Reputation:	low

Analysis Process: dNeoJAgJU5.exe PID: 6880 Parent PID: 7144

General

Start time:	09:02:55
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe
Imagebase:	0x4e0000
File size:	542192 bytes
MD5 hash:	D2A8EF4A18E3C6DC377DAF765B37A9CA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000000.795971862.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.847561501.0000000000EF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.847561501.0000000000EF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.847561501.0000000000EF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000000.795210062.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000002.846927570.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.795869224.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.795869224.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.795869224.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.846851933.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.846851933.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.846851933.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.848641291.0000000001250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.848641291.0000000001250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.848641291.0000000001250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6880

General

Start time:	09:02:57
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msdt.exe PID: 5724 Parent PID: 3424

General

Start time:	09:03:16
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x11a0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.909870472.0000000000EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.909870472.0000000000EA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.909870472.0000000000EA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.910711070.0000000004C80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.910711070.0000000004C80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.910711070.0000000004C80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.910650632.0000000004BF6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.911108077.000000000556F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.910769999.0000000004E10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.910769999.0000000004E10000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.910769999.0000000004E10000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 660 Parent PID: 5724

General

Start time:	09:03:20
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\dNeoJAgJU5.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4800 Parent PID: 660

General

Start time:	09:03:21
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 32.0.0 Black Diamond