ID: 552997
Sample Name: nji3Lg1ot6
Cookbook: default.jbs
Time: 03:36:23
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

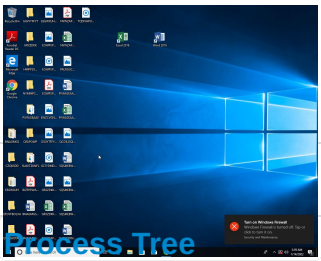
Windows Analysis Report nji3Lg1ot6

Overview

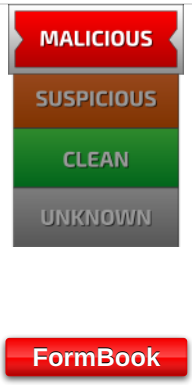
General Information

Sample Name:	nji3Lg1ot6 (renamed file extension from none to exe)
Analysis ID:	552997
MD5:	8eddcc35719034..
SHA1:	5506b69b4584f43.
SHA256:	0d072a60b433f33.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



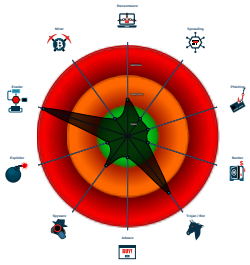
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- njI3Lg1ot6.exe (PID: 5092 cmdline: "C:\Users\user\Desktop\njI3Lg1ot6.exe" MD5: 8EDDCC35719034649F6947B2B08BCDF3)
  - njI3Lg1ot6.exe (PID: 6920 cmdline: "C:\Users\user\Desktop\njI3Lg1ot6.exe" MD5: 8EDDCC35719034649F6947B2B08BCDF3)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 6480 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
      - msiexec.exe (PID: 1304 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 7156 cmdline: /c del "C:\Users\user\Desktop\njI3Lg1ot6.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rthearts.com/nk6l/"
  ],
  "decoy": [
    "cbnextra.com",
    "entitysystemsinc.com",
    "55midwoodave.com",
    "ebelizzi.com",
    "khojcity.com",
    "1527brokenoakdrive.site",
    "housinghproperties.com",
    "ratiousa.com",
    "lrcrepresentacoes.net",
    "tocoec.net",
    "khadamatdemnate.com",
    "davidkastner.xyz",
    "gardeniaresort.com",
    "qiantangguoji.com",
    "visaprepaidprocessing.com",
    "cristinamadara.com",
    "semapisus.xyz",
    "mpwebagency.net",
    "alibabasdeli.com",
    "gigasupplies.com",
    "quantumskillset.com",
    "eajui136.xyz",
    "patsanchezelpaso.com",
    "trined.mobi",
    "amaturz.info",
    "approveprvqsx.xyz",
    "fronterapost.house",
    "clairewashere.site",
    "xn--3jst70hg8f.com",
    "thursdaynightthriller.com",
    "primacykapjlt.xyz",
    "vaginette.site",
    "olitusd.com",
    "paypal-caseid521.com",
    "preose.xyz",
    "ferbsqlv28.club",
    "iffiliatefreedom.com",
    "okdahotel.com",
    "cochuzyan.xyz",
    "hotyachts.net",
    "diamond-beauties.com",
    "storyofsol.com",
    "xianshucai.net",
    "venusmedicalarts.com",
    "energiaorgonu.com",
    "savannah.biz",
    "poeticdaily.com",
    "wilddalmatian.com",
    "kdydkyqksqucyuyen.com",
    "meanmod.xyz",
    "kaka.digital",
    "viewcision.com",
    "wowzerbackupandrestore-us.com",
    "hydrogendatapower.com",
    "427521.com",
    "ponto-bras.space",
    "chevalsk.com",
    "hnftdl.com",
    "nanasyhogar.com",
    "createacarepack.com",
    "wildkraeuter-wochenende.com",
    "uchihomedeco.com",
    "quintongiang.com",
    "mnbvending.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.344927446.00000000009C0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.344927446.00000000009C0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.344927446.00000000009C0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000000.316886950.000000000FFA5000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.316886950.000000000FFA5000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x191f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x40c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x7917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x891a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.nji3Lg1ot6.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.nji3Lg1ot6.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.0.nji3Lg1ot6.exe.400000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
1.2.nji3Lg1ot6.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.nji3Lg1ot6.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

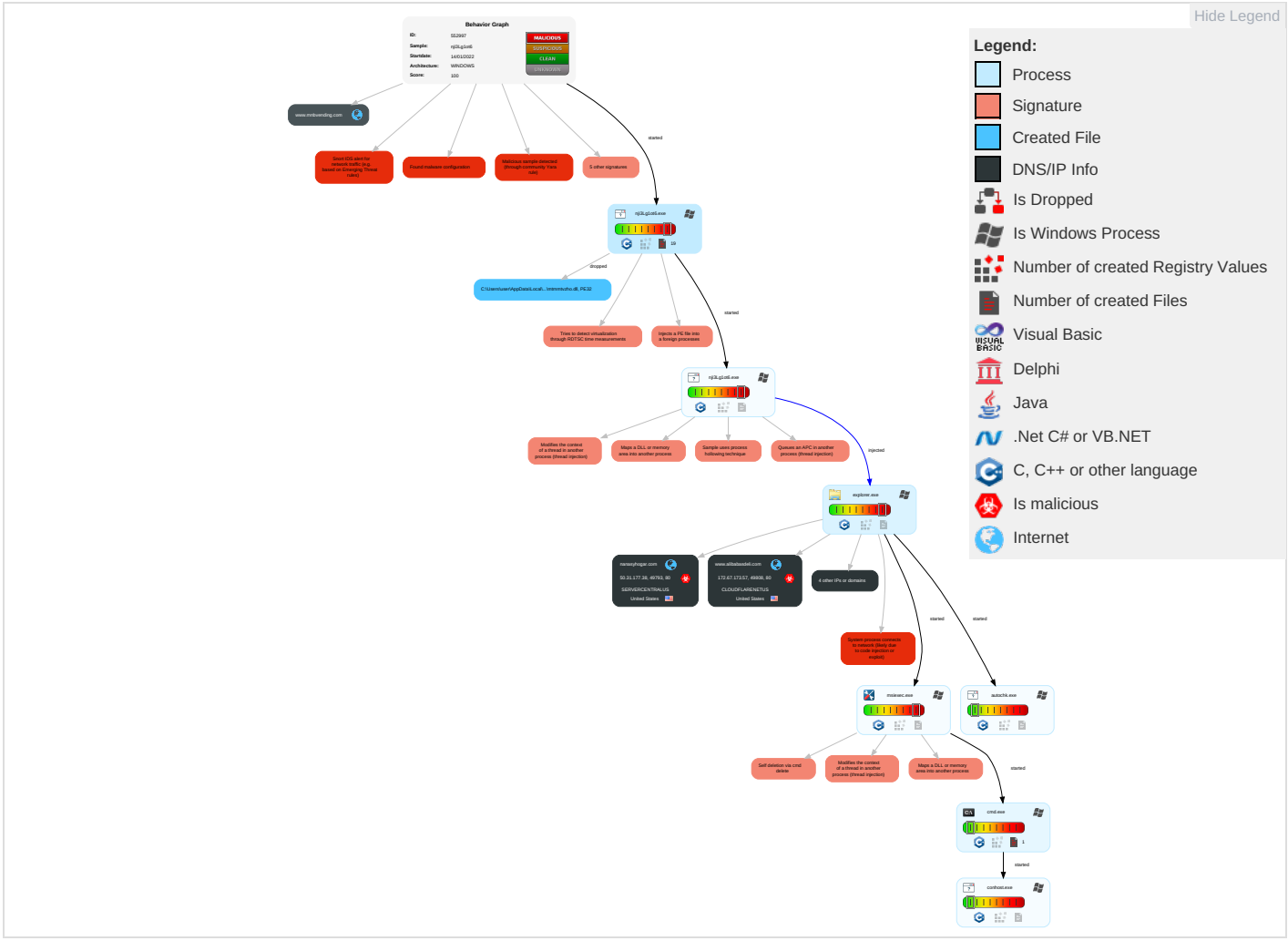
Yara detected FormBook

Remote Access Functionality:

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	Native API 1	DLL Side-Loading 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	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	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

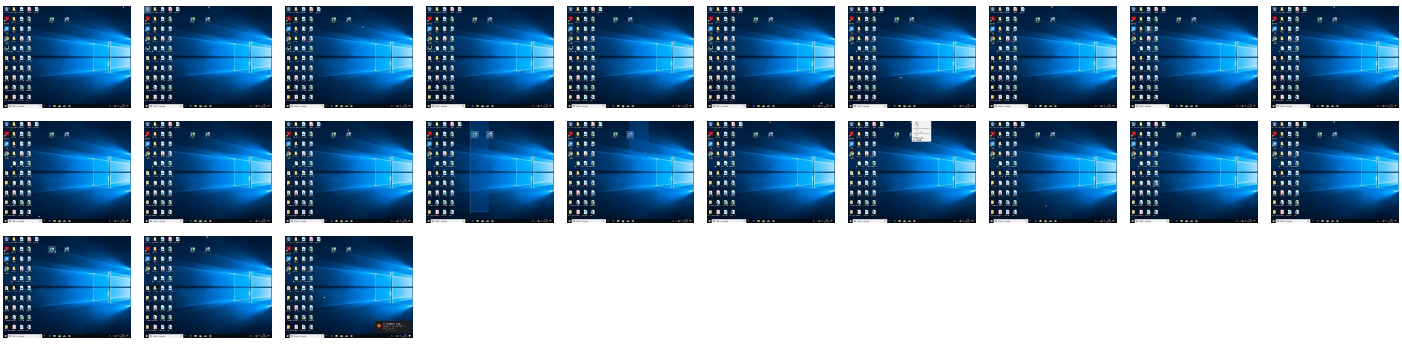
Behavior Graph



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
nji3Lg1ot6.exe	38%	Virustotal		Browse
nji3Lg1ot6.exe	42%	ReversingLabs	Win32.Worm.SpyBot	
nji3Lg1ot6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.msiexec.exe.4baf840.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.msiexec.exe.2c5b358.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.nji3Lg1ot6.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.nji3Lg1ot6.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nji3Lg1ot6.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.nji3Lg1ot6.exe.23e0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nji3Lg1ot6.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.nji3Lg1ot6.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Domains

Source	Detection	Scanner	Label	Link
www.mnbvending.com	0%	Virustotal		Browse
www.alibabasdeli.com	0%	Virustotal		Browse
shops.myshopify.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.nanasyhogar.com/nk6l/?Mn6p=MMWPsHlVo7vbxfqT+E8iHGCJx4EpOMO7XTm/RW/7WjycdebsiPyF7OJFYt5Z76O5OpDL&m87=kDHx4bf	0%	Avira URL Cloud	safe	
www.rthearts.com/nk6l/	0%	Avira URL Cloud	safe	
http://www.alibabasdeli.com/nk6l/?Mn6p=zX7TWLgUTNDtCnt/XwnHS79HNPNEveCsoMI9+/ObXOF7SG2tu7bFQ30QzdtJgFVEPE8r&m87=kDHx4bf	0%	Avira URL Cloud	safe	
http://www.gigasupplies.com/nk6l/?Mn6p=sMbkpElYm7OVlcdzrpiwDTFtc4P6BDcndIa3bMJ3nzzEqPK8OVYh2AVyK3PkcpAP2wum&m87=kDHx4bf	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mnbvending.com	199.59.243.200	true	false	• 0%, Virustotal, Browse	unknown
www.alibabasdeli.com	172.67.173.57	true	true	• 0%, Virustotal, Browse	unknown
nanasyhogar.com	50.31.177.38	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true	• 1%, Virustotal, Browse	unknown
www.nanasyhogar.com	unknown	unknown	true		unknown
www.gigasupplies.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.nanasyhogar.com/nk6l/?Mn6p=MMWPsHlVo7vbxfqT+E8iHGCJx4EpOMO7XTm/RW/7WjycdebsiPyF7OJFYt5Z76O5OpDL&m87=kDHx4bf	true	• Avira URL Cloud: safe	unknown
www.rthearts.com/nk6l/	true	• Avira URL Cloud: safe	low
http://www.alibabasdeli.com/nk6l/?Mn6p=zX7TWLgUTNDtCnt/XwnHS79HNPNEveCsoMI9+/ObXOF7SG2tu7bFQ30QzdtJgFVEPE8r&m87=kDHx4bf	true	• Avira URL Cloud: safe	unknown
http://www.gigasupplies.com/nk6l/?Mn6p=sMbkpElYm7OVlcdzrpiwDTFtc4P6BDcndIa3bMJ3nzzEqPK8OVYh2AVyK3PkcpAP2wum&m87=kDHx4bf	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.173.57	www.alibabasdeli.com	United States		13335	CLOUDFLARENETUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
50.31.177.38	nanasyhogar.com	United States		23352	SERVERCENTRALUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552997
Start date:	14.01.2022
Start time:	03:36:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nji3Lg1ot6 (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:	21
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@8/4@4/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.2% (good quality ratio 21.8%) • Quality average: 74.1% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 86% • 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\Temp\nsx7FAE.tmp	
Process:	C:\Users\user\Desktop\nji3Lg1ot6.exe
File Type:	data
Category:	dropped
Size (bytes):	252172
Entropy (8bit):	7.750682379260983
Encrypted:	false
SSDEEP:	6144:118MKS5foIrwbBl2/IO4cwyjICBga9xtqS+W:0MKS5pwdQIC99xtqA
MD5:	8644B9AA55DCA97B4841D7C3878444C7
SHA1:	1B7CD31D5C9509868830982D39D9A3F75B7E3AD4
SHA-256:	C41772CB8BD860959A61F832E221F9DC634BEBD8FE4CD141E45321E348EB4181
SHA-512:	2DEE50DCEDF000EC57222C3D12B30F7905B18977C929C14517A0DC2937DA7B6CFF0D7FBB093059AE5607AB3C3341C856FEACD4CFAC23C89F20EBBFD50B174 13
Malicious:	false
Reputation:	low
Preview:	.X.....,.....,C.....X.....X..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsx7FAF.tmp\mtmmtvzho.dll	
Process:	C:\Users\user\Desktop\nji3Lg1ot6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.8072208508576035
Encrypted:	false
SSDEEP:	24:e31GSNNCc0teIAUdax/+TCA5dieD4ueeDFE8hueeYoNXs+f3SlLRQ0K7ABPnRuVL:CnC/I9GTxieBJInFbfGFN1RuqS
MD5:	D62257B9F46BB3ECC454D94B80E839E8
SHA1:	A33070571B7909CEB589F9CCEB8591EE2DAE5C9F
SHA-256:	9679F0E8F63974D80F953B8212B2668C27EC9762CDCF6ACBFD4FDF4B6D189F23
SHA-512:	065531AFC2DA7DD6CECC893C13E41A1F15E0FC670E0DDC006E6F87CF5CB7A9B94D36275D2050953A11350590AC4D1B1B5FB89ACAA3C6B1F3F6C466D5E155F 07
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C] Rich..C].....PE..L.....a.....!..... .....P.....@..... ..H.... .....0.....@..<..... .....text...Q..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\pawgjsvu	
Process:	C:\Users\user\Desktop\nji3Lg1ot6.exe
File Type:	data
Category:	dropped
Size (bytes):	4769
Entropy (8bit):	6.209190395428905
Encrypted:	false
SSDEEP:	96:/s3+C1lu78g/85QphY5tVXUcbaLrVJ83Z/Lj+HNdC+cR3Sc3owy8WwXfUE/gmc01:i+CW8Q85ghY5tVkcbkU3hFdowyPwPUEX
MD5:	2CF23E8F99E539C2CFA7DF0709FFE950
SHA1:	B0DEF49E4CA1DE39D60696FFEC5EC6ECB9399D3C
SHA-256:	C71C94E4AA37C19EE3E62E4F20D03CE4950D9B7BCA8755B3729CBDB7897B6FDE
SHA-512:	0A028931CFE2F89C9324BA125DDFE576051CE68AFE556700D89EB74F0EC19DDBE1AB2C2E7AE96523CE231B47A18E5DB4935EF22E68F8708BC7663060F888D11 E

C:\Users\user\AppData\Local\Temp\pawgjsvu	
Malicious:	false
Reputation:	low
Preview:	..aa\2...!zOV.,.a.V....L..V....L..,.a.LUiaaa.,.a^<.^<.4L.q.daaa(L.(\u^<.^<.4L.q..aaa(L.(\.^<.^<.4L.q..aaa(L.(\.^<.^<.4L.q..aaa(L.(\...]/+[.YR.jjL..(L.(\}2L..]..(L.(t.2L.2tU4]...[.. ..2L.j\U4].(LUVO(,..}.[..aaaa.]=..,U^<..^<..^<. Y^<. .^<..^<....M.&I2..&I(e.A..`<.^<. .2L...(L.j,U.aaaa..=]Jaaa.]=..2,...2L....2...a\2.pp.V....L.2L.2a"L.ZA2L.2a2t.2..(\.2..](LU2L.2 a!2t.(`2L.2\U2...a).k..9.aa.G.aa.a).^~...aa...aa.a)....m.aa.{.aa.a\2...i.V....L..L..aaa4L.(LU..aM.2LU.aa2LU!(LU2L.I(L..}...aa..M?2L..[..R.a(...(m.u4L..[....a(...(m.u[.[.YR.a4...q). ^~..`aaq..d^^(L..4L.q^<..{^^^(L....aM..,.a..L.`aaa2L.2...]a\2...!.V....L..L.iaaa4L.(LU..aM.2LU.aa2LU!(LU2L.I(L..}.]aa....;aaa2L..[..R.a(...(m..2L..[....a(...(m..2L..[....(...(m..2L... [..R.j(...(e..4L..[.....(...(m..[.[.YR.a4...q).k...aaaq..U^^(L...aM.2L.2t.(`.^<.^<.^<.^<.^<..vW^^(L....aM..,.a..L.`aaa2L.2...a\2...5.L..aaa4L}(LU..aM.2LU.aa2LU!(LU2L.I(L..}.[jaa..M? 2L..[..R.a(..}(m..2L..[....a(..}(m..[.[.YR.a4..}q)....faaaq.=U^^(L..^<

C:\Users\user\AppData\Local\Temp\zn2eyxxq9ww5zrdhr	
Process:	C:\Users\user\Desktop\nji3Lg1ot6.exe
File Type:	data
Category:	dropped
Size (bytes):	220020
Entropy (8bit):	**7.992864927984938**
Encrypted:	**true**
SSDEEP:	6144:7MKS5foIrwbBl2/IO4cwyjICBga9xtqS+Wx:7MKS5pwdQIC99xtqAx
MD5:	A75D055E6FABC0D24984208FC2BD8877
SHA1:	F4071D8B3141A30FC0D70787D174B8E31C6131FC
SHA-256:	6497E85685A07951F80AE543BB730D7714717596140569E4D5C9388F2E6CBE59
SHA-512:	3A09EEF95C13AF84D71512DBFCDB2C6D87412844443411E2235E47797E9582A12FEA44848E1037B7C56C60E233CC2EA962E59BEE917F13C60103B2B196A51F4E
Malicious:	false
Reputation:	low
Preview:	.....r_..oJ...Pae...w.;.z..o../"j...p.$(<h...g....=.}4..y_e..+;...y...r.....Q..._..p5$...q.....D..@....1...>G.`.OY...2.t=.)....o.....[P.u.>q.?O.....h..q.....0.).Jn..%..r.M.....U...,4.T.!/..... .N^.....d....Kqt1G..G...;...k)`=@.Ow.>I.....vf.eF.....:S...-"../"c...p.$(.h...g.,..=.}4..y_;!..;...`..Hc..e.|c.8...0..O|..D.h.Q.....^*"...i3....`.`.OY..F.....k8.V...D..4..ML$.....bQ...m{.....uw .;^...0.).|.].E..r.H..G...A,.T.!/.....V.h.....d..H.Kq[1G.....k)`D@.Qw.>I..r.....v..eFR...:S.+..o../"j...p.$(<h...g....=.}4..y_;!..;...`..Hc..e.|c.8...0..O|..D.h.Q.....^*"...i3....`.`.OY..F... ...k8.V...D..4..ML$.....bQ...m{.....uw.;^...0.).Jn..%..r,...G..m.A,4.T.!/.....NV.....d..H.Kq[1G.....k)`D@.Qw.>I..r.....v..eFR...:S.+..o../"j...p.$(<h...g....=.}4..y_;!..;...`..Hc.. e.|c.8...0..O|..D.h.Q.....^*"...i3....`.`.OY..F.....k8.V...D..4..ML$.....bQ...m{.....uw.;^...0.).Jn..%..r,...G..m.A,4.T.!/.....NV.....d.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.927911380419802
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	nji3Lg1ot6.exe
File size:	248302
MD5:	8eddcc35719034649f6947b2b08bcdf3
SHA1:	5506b69b4584f43232f45299192a540ec0197998
SHA256:	0d072a60b433f330d2ba97d75eae7af07e9d75bc6ed5b1(65287661d05e82ab6
SHA512:	c7716daafffd44dff6143d7fe0fb686eb5fc08da918aab204 ae6d7c8687dc914d9310d488a2ffc4767e5fd643e8aee6d 88fadf28d156c6be731c29bcc3943681
SSDEEP:	6144:owzN+wRSsYU12O6NgFRQbIuoKFFmhmvk8nw:fN+w8KCWRbRKF7vkR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-03:39:09.329226	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.2.3	23.227.38.74
01/14/22-03:39:09.329226	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.2.3	23.227.38.74

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-03:39:09.329226	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.2.3	23.227.38.74
01/14/22-03:39:09.373367	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49819	23.227.38.74	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 03:38:27.518068075 CET	192.168.2.3	8.8.8.8	0x7cdd	Standard query (0)	www.nanasyhogar.com	A (IP address)	IN (0x0001)
Jan 14, 2022 03:38:48.632225037 CET	192.168.2.3	8.8.8.8	0x7e08	Standard query (0)	www.alibabasdeli.com	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:09.281239986 CET	192.168.2.3	8.8.8.8	0xd5ac	Standard query (0)	www.gigasupplies.com	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:29.496071100 CET	192.168.2.3	8.8.8.8	0x1d40	Standard query (0)	www.mnbvending.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 03:38:27.765955925 CET	8.8.8.8	192.168.2.3	0x7cdd	No error (0)	www.nanasyhogar.com	nanasyhogar.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 03:38:27.765955925 CET	8.8.8.8	192.168.2.3	0x7cdd	No error (0)	nanasyhogar.com		50.31.177.38	A (IP address)	IN (0x0001)
Jan 14, 2022 03:38:48.656395912 CET	8.8.8.8	192.168.2.3	0x7e08	No error (0)	www.alibabasdeli.com		172.67.173.57	A (IP address)	IN (0x0001)
Jan 14, 2022 03:38:48.656395912 CET	8.8.8.8	192.168.2.3	0x7e08	No error (0)	www.alibabasdeli.com		104.21.30.160	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:09.309283972 CET	8.8.8.8	192.168.2.3	0xd5ac	No error (0)	www.gigasupplies.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 03:39:09.309283972 CET	8.8.8.8	192.168.2.3	0xd5ac	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jan 14, 2022 03:39:29.602072954 CET	8.8.8.8	192.168.2.3	0x1d40	No error (0)	www.mnbvending.com		199.59.243.200	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.nanasyhogar.com
- www.alibabasdeli.com
- www.gigasupplies.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49793	50.31.177.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 03:38:27.889576912 CET	10300	OUT	GET /nk6l/?Mn6p=MMWPsHlVo7vbxfqT+E8iHGCJx4EpOMO7XTm/RW/7WjycdebsiPyF7OJFYt5Z76O5OpDL&m87=kDHx4bf HTTP/1.1 Host: www.nanasyhogar.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 03:38:28.461199999 CET	10301	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 x-redirect-by: WordPress location: https://www.nanasyhogar.com/nk6l/?Mn6p=MMWPsHlVo7vbxfqT+E8iHGCJx4EpOMO7XTm/RW/7WjycdebsiPyF7OJFYt5Z76O5OpDL&m87=kDHx4bf content-length: 0 date: Fri, 14 Jan 2022 02:38:27 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49808	172.67.173.57	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 03:38:48.677973032 CET	12054	OUT	GET /nk6l/?Mn6p=zX7TWLgUTNDtCnt/XwnHS79HNPNEveCsoMI9+/ObXOF7SG2tu7bFQ30QzdtJgFVEPE8r&m87=kDHx4bf HTTP/1.1 Host: www.alibabasdeli.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 03:38:48.705641031 CET	12055	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 14 Jan 2022 02:38:48 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 14 Jan 2022 03:38:48 GMT Location: https://www.alibabasdeli.com/nk6l/?Mn6p=zX7TWLgUTNDtCnt/XwnHS79HNPNEveCsoMI9+/ObXOF7SG2tu7bFQ30QzdtJgFVEPE8r&m87=kDHx4bf Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=IgjFfWdmsLKF6nMy5eaecanBpYGYtijY%2F9ML7bYbo0jwULbFmirtMXIUFdaeYKaZw0SjcZLe8AgxrbUYROuDN%2FNsw420lPpE5m2qvu%2BdTZvcH%2BD2gpXk494OMVi7AvX9wFxVMZB9xg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd37d8248424df4-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49819	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 03:39:09.329226017 CET	12088	OUT	GET /nk6l/?Mn6p=sMbkpElYm7OVlcdzrpiwDTFtc4P6BDcndIa3bMJ3nzzEqPK8OVYh2AVyK3PkcpAP2wum&m87=kDHx4bf HTTP/1.1 Host: www.gigasupplies.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 03:39:09.373367071 CET	12089	IN	HTTP/1.1 403 Forbidden Date: Fri, 14 Jan 2022 02:39:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 188 X-Sorting-Hat-ShopId: 60258091197 X-Dc: gcp-europe-west1 X-Request-ID: 077675b5-2854-474a-9745-e2e99dc925ce X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6cd37e035a694e0e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:col

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: nji3Lg1ot6.exe PID: 5092 Parent PID: 3160

General

Start time:	03:37:19
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\nji3Lg1ot6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nji3Lg1ot6.exe"
Imagebase:	0x400000
File size:	248302 bytes
MD5 hash:	8EDDCC35719034649F6947B2B08BCDF3
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: 00000000.00000002.295727882.00000000023E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.295727882.00000000023E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.295727882.00000000023E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: nji3Lg1ot6.exe PID: 6920 Parent PID: 5092

General

Start time:	03:37:20
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\nji3Lg1ot6.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\nji3Lg1ot6.exe"
Imagebase:	0x400000
File size:	248302 bytes
MD5 hash:	8EDDCC35719034649F6947B2B08BCDF3
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: 00000001.00000002.344927446.00000000009C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.344927446.00000000009C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.344927446.00000000009C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.292323567.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.292323567.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.292323567.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.345328799.0000000000D30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.345328799.0000000000D30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.345328799.0000000000D30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.344714240.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.344714240.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.344714240.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.294869944.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.294869944.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.294869944.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.293866561.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.293866561.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.293866561.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 6920

General

Start time:	03:37:23
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.316886950.000000000FFA5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.316886950.000000000FFA5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.316886950.000000000FFA5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.333023210.000000000FFA5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.333023210.000000000FFA5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.333023210.000000000FFA5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autochk.exe PID: 6480 Parent PID: 3352

General

Start time:	03:37:42
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0xdc0000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msiexec.exe PID: 1304 Parent PID: 3352

General

Start time:	03:37:42
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x890000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.556861627.00000000006C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.556861627.00000000006C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.556861627.00000000006C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.562054407.0000000002920000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.562054407.0000000002920000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.562054407.0000000002920000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.561888247.00000000028F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.561888247.00000000028F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.561888247.00000000028F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7156 Parent PID: 1304

General

Start time:	03:37:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\nji3Lg1ot6.exe"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5352 Parent PID: 7156

General

Start time:	03:37:47
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis