ID: 458885
Sample Name: Shipping
Doc.exe
Cookbook: default.jbs
Time: 20:39:22
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

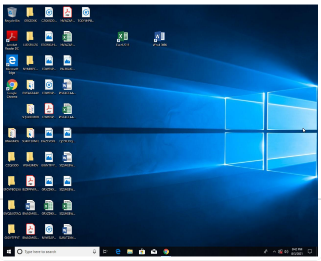
Windows Analysis Report Shipping Doc.exe

Overview

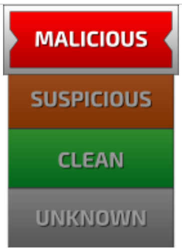
General Information

Sample Name:	Shipping Doc.exe
Analysis ID:	458885
MD5:	159d560ff64cdb2..
SHA1:	5762036dd01f8a6.
SHA256:	065252f5ed5475c.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



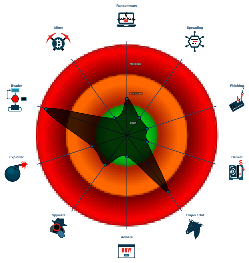
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- Shipping Doc.exe (PID: 1932 cmdline: 'C:\Users\user\Desktop\Shipping Doc.exe' MD5: 159D560FF64CDB2D130B1635F4123A49)
  - Shipping Doc.exe (PID: 2148 cmdline: C:\Users\user\Desktop\Shipping Doc.exe MD5: 159D560FF64CDB2D130B1635F4123A49)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 2000 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 3984 cmdline: /c del 'C:\Users\user\Desktop\Shipping Doc.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.shopjempress.com/amb6/"
  ],
  "decoy": [
    "segurocars.com",
    "rylautosales.com",
    "xinglinjiankang.com",
    "dantil-brand.com",
    "sofaloffa.club",
    "coinclub2.com",
    "ez-pens.com",
    "gqtlqsw.com",
    "robotnewswire.com",
    "ktproductreviews.com",
    "merchbrander.com",
    "yesonamendmentb.com",
    "losgatoslimos.com",
    "kristincole.art",
    "metalmaids.online",
    "leftcoastmodels.com",
    "athetheist.com",
    "jblbusrtingsale.com",
    "chungcugiarehcm.com",
    "renblockchain.com",
    "bigdaddy.fish",
    "comproliverton.pro",
    "gzmove.com",
    "honeythymeherbfarm.com",
    "davinescosmetics.com",
    "9355693.com",
    "movinmemphis901.com",
    "patriotsrs.net",
    "dagelijkseschoenen.com",
    "a-want-ad.site",
    "theodbox.com",
    "audioky.net",
    "hopematthewsrealtor.com",
    "theonlinemoneymachine.com",
    "misakiti.com",
    "ad-yalong.com",
    "mikealazo.com",
    "marianoterra.com",
    "shivorja.com",
    "goodvibrationswindchimes.com",
    "pecom-deliverry.online",
    "amlexcel.com",
    "emeralddrumcompany.com",
    "dalipaella.com",
    "shopcamacci.com",
    "xucaiwujin.com",
    "bxs5000.com",
    "2en1institut.com",
    "zxzm47-wj.com",
    "builttek.com",
    "66400yy.com",
    "beegraze.com",
    "thedottedcat.com",
    "komsah.com",
    "4202nsacramentoav.info",
    "88q27.com",
    "toriengenharia.com",
    "briscoewelding.com",
    "brookelenzi.com",
    "tribaltrash.com",
    "bidtas.com",
    "shokhorror.com",
    "bodurm.com",
    "333.wiki"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.480234994.0000000005230000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.480234994.0000000005230000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.480234994.0000000005230000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.320916195.0000000001C90000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.320916195.0000000001C90000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.Shipping Doc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.Shipping Doc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.Shipping Doc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
4.2.Shipping Doc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.Shipping Doc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
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

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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 virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

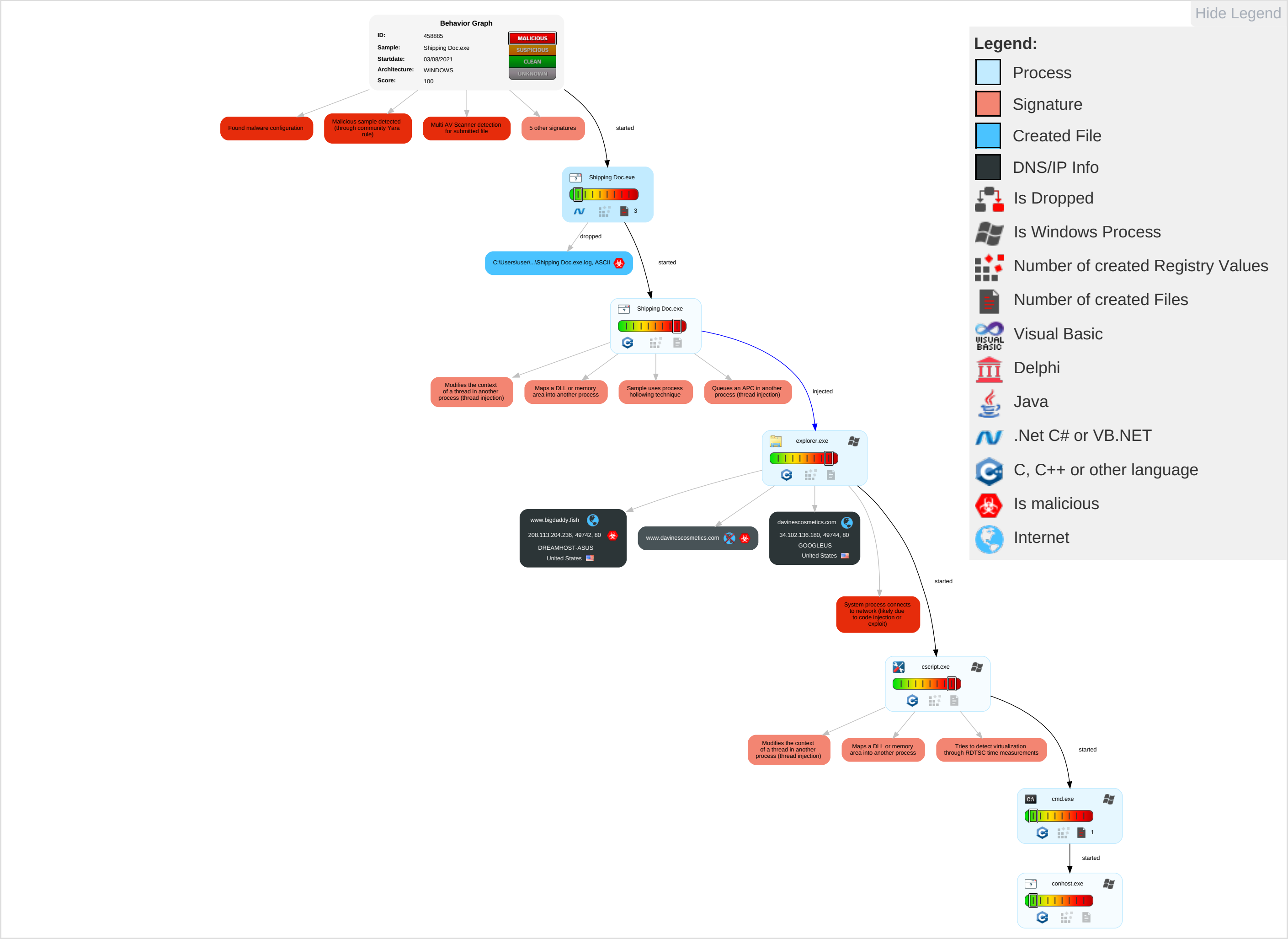
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
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 Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System 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 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

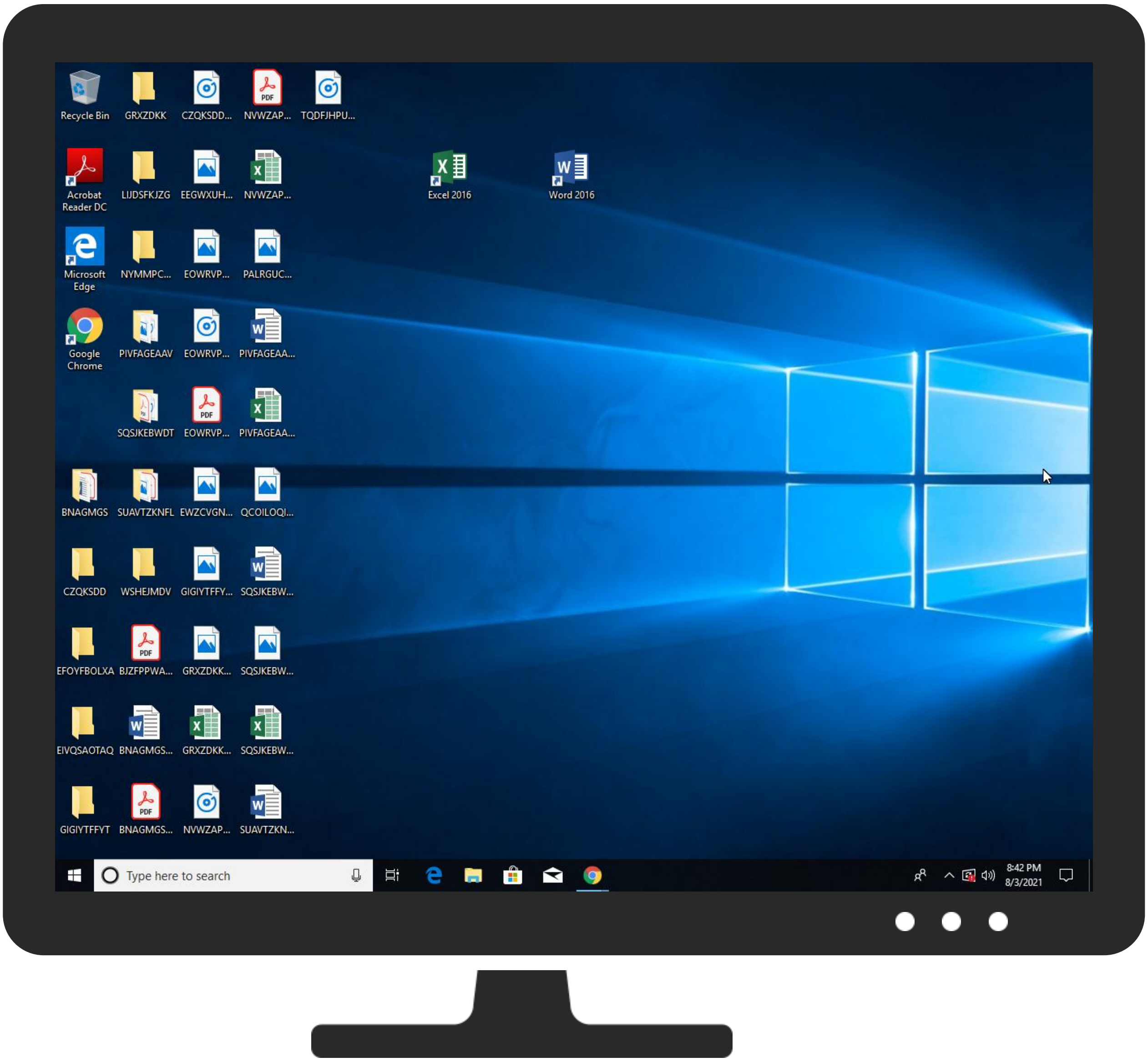
Behavior Graph


Behavior Graph
ID: 458885
Sample: Shipping Doc.exe
Startdate: 03/08/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Multi AV Scanner detection for submitted file
5 other signatures
started
Shipping Doc.exe
3
dropped
C:\Users\user\...\Shipping Doc.exe.log, ASCII
started
Shipping Doc.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
injected
explorer.exe
www.bigdaddy.fish
208.113.204.236, 49742, 80
DREAMHOST-ASUS
United States
www.davinescosmetics.com
davinescosmetics.com
34.102.136.180, 49744, 80
GOOGLEUS
United States
System process connects to network (likely due to code injection or exploit)
started
cscript.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
cmd.exe
1
started
conhost.exe
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Shipping Doc.exe	51%	Virustotal		Browse
Shipping Doc.exe	37%	Metadefender		Browse
Shipping Doc.exe	26%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
Shipping Doc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/argeg	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.founder.com.cn/cnP	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/vam&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/fr-f	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/siv	0%	URL Reputation	safe	
http://www.davinescosmetics.com/amb6/?DPt4=ZduBhxyNf/T8KdukIHnfIOdlFHQuF1EsUtpfZKs5gLBpa2z0TfcmffP3A+e7CMLv2uy0&l8B=RjAhR	0%	Avira URL Cloud	safe	
http://www.fonts.comny	0%	Avira URL Cloud	safe	
http://www.tiro.coml	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comcomFU	0%	Avira URL Cloud	safe	
http://www.typography.netD	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.jiyu-kobo.co.jp/en-u	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comalsdn	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.fontbureau.comlicd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cny	0%	URL Reputation	safe	
http://www.fonts.comicV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/0	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sakkal.comc	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0a	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coma7	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.bigdaddy.fish/amb6/?DPt4=by49o9P4nbuTuOEn2y8q30QOI4mC2WgRQPsTiLFqW4T5eczeXRV1KBHGOAlC+0HR5lXX&l8B=RjAhR	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
www.shopjempress.com/amb6/	0%	Avira URL Cloud	safe	
http://BigDaddyUnlimited.com/amb6/?DPt4=by49o9P4nbuTuOEn2y8q30QOI4mC2WgRQPsTiLFqW4T5eczeXRV1KBHGOAlC	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/n	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/q	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	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.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.founder.com.cn/cn&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/en-ut	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bigdaddy.fish	208.113.204.236	true	true		unknown
davinescosmetics.com	34.102.136.180	true	false		unknown
www.davinescosmetics.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.davinescosmetics.com/amb6/?DPt4=ZduBhxyNf/T8KdukIHnflOdlFHQuF1EsUtpfZKs5gLBpa2z0TfcmffP3A+e7CMLv2uy0&l8B=RjAhR	false	• Avira URL Cloud: safe	unknown
http://www.bigdaddy.fish/amb6/?DPt4=by49o9P4nbuTuOEn2y8q30QOI4mC2WgRQPsTiLFqW4T5eczeXRV1KBHGOAlC+0HR5lXX&l8B=RjAhR	true	• Avira URL Cloud: safe	unknown
www.shopjempress.com/amb6/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	davinescosmetics.com	United States	🇺🇸	15169	GOOGLEUS	false
208.113.204.236	www.bigdaddy.fish	United States	🇺🇸	26347	DREAMHOST-ASUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458885
Start date:	03.08.2021
Start time:	20:39:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping Doc.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:	24
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@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 67.2% (good quality ratio 62.1%) • Quality average: 69.6% • Quality standard deviation: 31.4%

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
20:40:34	API Interceptor	1x Sleep call for process: Shipping Doc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DREAMHOST-ASUS	ORDER_0009_PDF.exe	Get hash	malicious	Browse	- 69.163.167.176
	A77HHPWkxJ.dll	Get hash	malicious	Browse	- 208.113.160.88
	YaRh8PG41y.exe	Get hash	malicious	Browse	- 69.163.228.182
	uw01Qp8GcO.exe	Get hash	malicious	Browse	- 69.163.228.182
	PAYMENT_COPY.exe	Get hash	malicious	Browse	- 69.163.224.143
	Order-CNS Amura Precision Co., Ltd 9A210118KR.exe	Get hash	malicious	Browse	- 69.163.224.174
	USD980950_Swift.exe	Get hash	malicious	Browse	- 173.236.228.194
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	- 69.163.224.174
	HSBCpaymentSlipPDF.exe	Get hash	malicious	Browse	- 69.163.226.116
	NEW ORDER.xlsx	Get hash	malicious	Browse	- 75.119.198.195
	Order_1537-25.exe	Get hash	malicious	Browse	- 208.113.197.232
	Order 5122948.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	Order 5122948.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	INS 0966828.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	Order 2522592.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	INS 0966828.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	Order 2522592.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	INS 53614716.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	WO 2825876.xlsb	Get hash	malicious	Browse	- 64.111.126.83
	INS 53614716.xlsb	Get hash	malicious	Browse	- 64.111.126.83

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Shipping Doc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	high, very likely benign file
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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):	7.195385958745407
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	Shipping Doc.exe
File size:	1037312
MD5:	159d560ff64cdb2d130b1635f4123a49
SHA1:	5762036dd01f8a63ce29557c5c0464360500c7e6
SHA256:	065252f5ed5475c89d2bff7389554a4695a85900a7a75eb98170c6a372b33ea0
SHA512:	be415739b37b83d24c0d097680ddc2450be5de89f0b844c4b9790c039626f79ffac32f006b9c0febe37c84c519c703c65e03d2648c836b1f0dcd404c0026c4a6
SSDEEP:	24576:XB8ns9/deerxEjxbzXDusP8z5y8dWImtw:X4TuDcDImC
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....H..............................~.... ....@.. ....@............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4fe87e

General

Entrypoint Section:	.text
Digitally signed:	false
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:	0xAAC44811 [Thu Oct 14 14:37:05 2060 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	0xfc884	0xfca00	False	0.696450937036	data	7.2014231354	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x100000	0x5d8	0x600	False	0.4296875	data	4.13984531351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x102000	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
08/03/21-20:42:09.835215	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49744	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:41:48.954216957 CEST	192.168.2.3	8.8.8.8	0xe08b	Standard query (0)	www.bigdaddy.fish	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:09.661616087 CEST	192.168.2.3	8.8.8.8	0x9ec5	Standard query (0)	www.davinescosmetics.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:41:49.091502905 CEST	8.8.8.8	192.168.2.3	0xe08b	No error (0)	www.bigdaddy.fish		208.113.204.236	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:09.698745966 CEST	8.8.8.8	192.168.2.3	0x9ec5	No error (0)	www.davinescosmetics.com	davinescosmetics.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:42:09.698745966 CEST	8.8.8.8	192.168.2.3	0x9ec5	No error (0)	davinescosmetics.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.bigdaddy.fish
- www.davinescosmetics.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	208.113.204.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:41:49.208802938 CEST	6582	OUT	GET /amb6/?DPt4=by49o9P4nbuTuOEn2y8q30QOI4mC2WgRQPsTiLFqW4T5eczeXRV1KBHGOAlC+0HR5lXX&l8B=RjAhR HTTP/1.1 Host: www.bigdaddy.fish Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 20:41:49.321682930 CEST	6582	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 03 Aug 2021 18:41:49 GMT Server: Apache Location: http://BigDaddyUnlimited.com/amb6/?DPt4=by49o9P4nbuTuOEn2y8q30QOI4mC2WgRQPsTiLFqW4T5eczeXRV1KBHGOAlC+0HR5lXX&l8B=RjAhR Content-Length: 330 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 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 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 42 69 67 44 61 64 64 79 55 6e 6c 69 6d 69 74 65 64 2e 63 6f 6d 2f 61 6d 62 36 2f 3f 44 50 74 34 3d 62 79 34 39 6f 39 50 34 6e 62 75 54 75 4f 45 6e 32 79 38 71 33 30 51 4f 49 34 6d 43 32 57 67 52 51 50 73 54 69 4c 46 71 57 34 54 35 65 63 7a 65 58 52 56 31 4b 42 48 47 4f 41 6c 43 2b 30 48 52 35 6c 58 58 26 61 6d 70 3b 6c 38 42 3d 52 6a 41 68 52 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body><h1>Moved Permanently</h1><p>The document has moved <a href="http://BigDaddyUnlimited.com/amb6/?DPt4=by49o9P4nbuTuOEn2y8q30QOI4mC2WgRQPsTiLFqW4T5eczeXRV1KBHGOAlC+0HR5lXX&amp;l8B=RjAhR">here</a>.</p></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:42:09.720345020 CEST	6593	OUT	GET /amb6/?DPt4=ZduBhxyNf/T8KdukIHnfIOdlFHQuF1EsUtpfZKs5gLBpa2z0TfcmffP3A+e7CMLv2uy0&l8B=RjAhR HTTP/1.1 Host: www.davinescosmetics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:42:09.835215092 CEST	6594	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 18:42:09 GMT Content-Type: text/html Content-Length: 275 ETag: "61048812-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 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 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 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 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body><h1>Access Forbidden</h1></body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Shipping Doc.exe PID: 1932 Parent PID: 5704

General

Start time:	20:40:13
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Shipping Doc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping Doc.exe'
Imagebase:	0x3b0000
File size:	1037312 bytes
MD5 hash:	159D560FF64CDB2D130B1635F4123A49
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: Shipping Doc.exe PID: 2148 Parent PID: 1932

General

Start time:	20:40:35
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Shipping Doc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Shipping Doc.exe
Imagebase:	0xe90000
File size:	1037312 bytes
MD5 hash:	159D560FF64CDB2D130B1635F4123A49
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: 00000004.00000002.320916195.0000000001C90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.320916195.0000000001C90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.320916195.0000000001C90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.320396445.00000000014D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.320396445.00000000014D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.320396445.00000000014D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.319900347.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.319900347.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.319900347.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 2148

General

Start time:	20:40:37
Start date:	03/08/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
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: cscript.exe PID: 2000 Parent PID: 3388

General

Start time:	20:41:03
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xde0000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 0000000F.00000002.480234994.0000000005230000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.480234994.0000000005230000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.480234994.0000000005230000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.478585925.0000000003200000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.478585925.0000000003200000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.478585925.0000000003200000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.479510604.0000000003830000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.479510604.0000000003830000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.479510604.0000000003830000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 3984 Parent PID: 2000

General

Start time:	20:41:06

Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Shipping Doc.exe'
Imagebase:	0xbd0000
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: 6040 Parent PID: 3984

General

Start time:	20:41:06
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond