ID: 458954
Sample Name:
Payment_Advice.exe
Cookbook: default.jbs
Time: 22:30:20
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

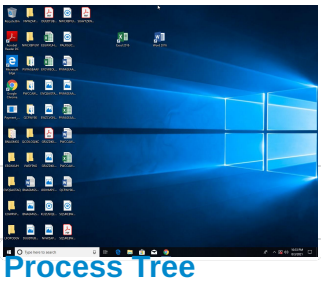
Windows Analysis Report Payment_Advice.exe

Overview

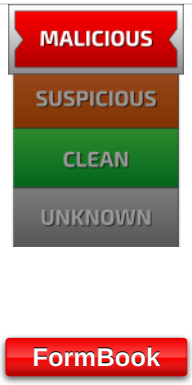
General Information

Sample Name:	Payment_Advice.exe
Analysis ID:	458954
MD5:	b5a3a16559c14a..
SHA1:	31280391b1a399..
SHA256:	c8ff043caee4e9c...
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



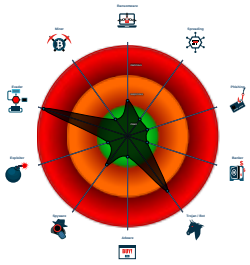
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through ...
- Multi AV Scanner detection for subm...
- Snort IDS alert for network traffic (e....
- System process connects to networ...
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia...
- .NET source code contains very larg...
- Allocates memory in foreign process...
- C2 URLs / IPs found in malware con...
- Initial sample is a PE file and has a ...

Classification



Process Tree

- **System is w10x64**
- Payment_Advice.exe (PID: 2648 cmdline: 'C:\Users\user\Desktop\Payment_Advice.exe' MD5: B5A3A16559C14A2DB6837FB8792134AE)
  - RegSvcs.exe (PID: 1156 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
    - cmd.exe (PID: 2288 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5756 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 2344 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 1156 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.illoftapartments.com/uecu/"
  ],
  "decoy": [
    "ishtarhotel.com",
    "woodstrends.icu",
    "jalenowens.com",
    "manno.expert",
    "ssg1asia.com",
    "telepathylaw.com",
    "quickoprintnv.com",
    "abrosnm3.com",
    "lumberjackcatering.com",
    "beachujamaica.com",
    "thomasjeffersonbyrd.com",
    "starryfinds.com",
    "shelavish2.com",
    "royalglamempirellc.com",
    "deixandomeuemprego.com",
    "alexgoestech.xyz",
    "opticamn.com",
    "fermanchevybrandon.com",
    "milbodegas.info",
    "adunarsrl.com",
    "dataatlus.com",
    "missabrams.com",
    "beaconservicesuk.com",
    "tvforpc.website",
    "dipmarketingagency.com",
    "milsontt.com",
    "londonsashwindowsservices.com",
    "feedmysheepdaily.com",
    "firsttimephysics.com",
    "hosefire.com",
    "southdocknj.com",
    "idfstool.com",
    "drelip.com",
    "decayette.com",
    "awakenedgodsofbeauty.com",
    "easttexasranch.com",
    "risinglanka.com",
    "meetingoffices.com",
    "vase-composition.com",
    "kupon.asia",
    "alltimeselfstorage.com",
    "gatorbrewcoffee.com",
    "api-pay-agent.com",
    "height-project.online",
    "flbtyc638.com",
    "psdmoravita.com",
    "highbrowhairstudio.com",
    "deepblueriver.com",
    "yh22022.com",
    "sts-100.com",
    "michaelfmoore.com",
    "alzheimers.computer",
    "produtos-servicos.website",
    "zyuyktlcu.icu",
    "ezewasser.com",
    "outstanding-palisade.com",
    "saioura.com",
    "core.run",
    "allaboutlifeblog.com",
    "foodolog.net",
    "somerderm.com",
    "scootrlv.com",
    "ahjjbxg.com",
    "gasworldchampionships.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.355992168.0000000000A80000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.355992168.0000000000A80000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.355992168.0000000000A80000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.470886740.00000000025B0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.470886740.00000000025B0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
12.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
12.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

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)

Allocates memory in foreign processes

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

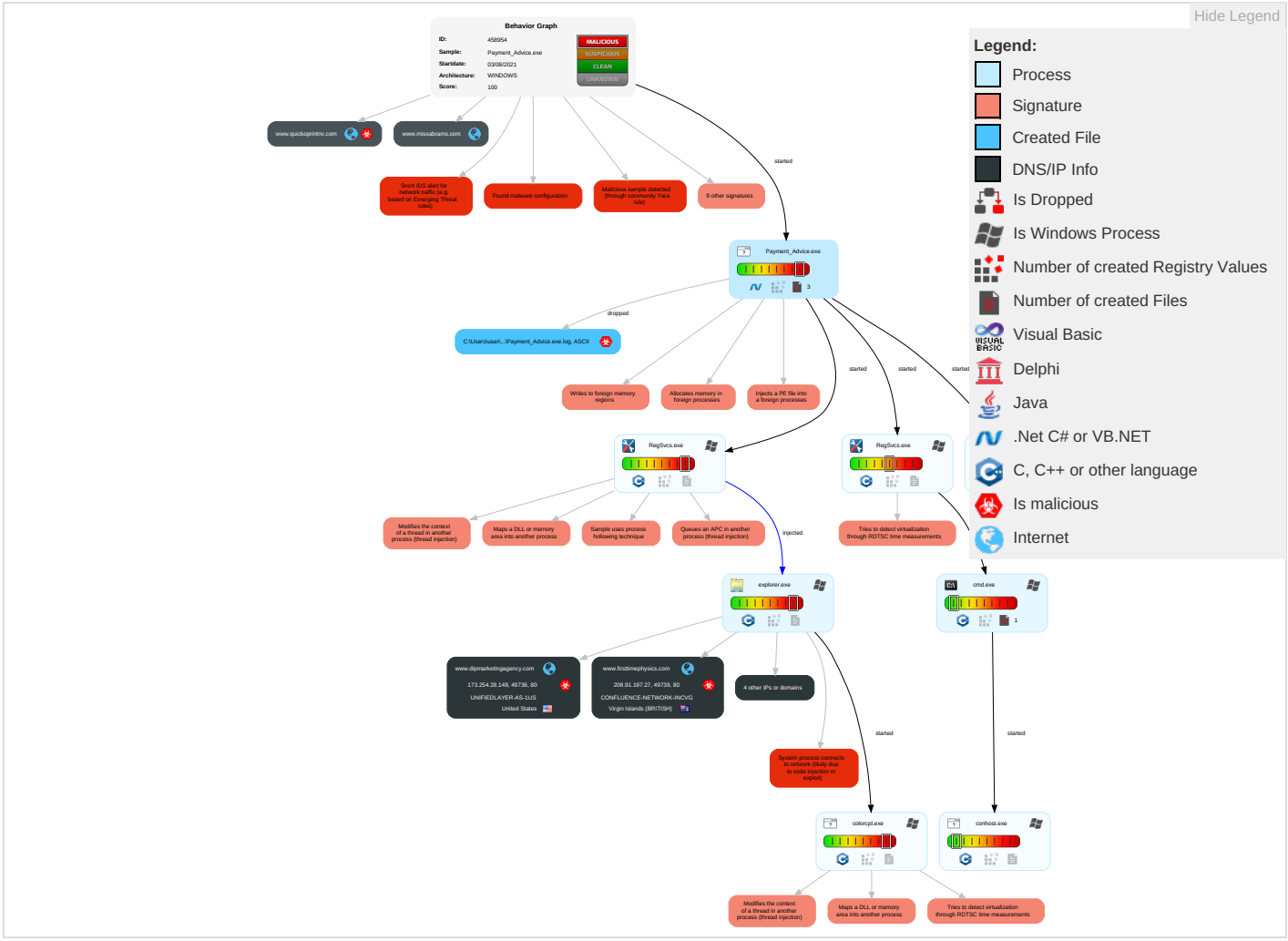
Remote Access Functionality:

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 8 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 8 1 2	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	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	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	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Payment_Advice.exe	43%	Virustotal		Browse
Payment_Advice.exe	46%	Metadefender		Browse
Payment_Advice.exe	86%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Payment_Advice.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
illoftapartments.com	2%	Virustotal		Browse
www.missabrams.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.illoftapartments.com/uecu/?2d3pCdLh=I+cFmvzvjfujRN3oltevYzRyUOJqDj5YxiqkJ4i7Zjmur1++tOYpTWGX3hXOvnB+KlCx&fXJ=z64Txz	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comamM	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comm%M	0%	Avira URL Cloud	safe	
http://www.arifureta-shokugyou-de-sekai-saikyou.com?fXJ=z64Txz&2d3pCdLh=euCGN8RtrYk2s603FqWaeKSKafFu	0%	Avira URL Cloud	safe	
http://www.firsttimephysics.com/uecu/?2d3pCdLh=hr7+JRYyT1HVyDshWD8v/2ivT/o36mEBRVmbpvRN6jTQqfRWnpyet8LANEukLjLgYMOr&fXJ=z64Txz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
www.illoftapartments.com/uecu/	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.dipmarketingagency.com	173.254.28.149	true	true		unknown
illoftapartments.com	34.102.136.180	true	false	• 2%, Virustotal, Browse	unknown
manno.expert	34.102.136.180	true	false		unknown
www.missabrams.com	45.197.108.106	true	false	• 0%, Virustotal, Browse	unknown
www.quickoprintnv.com	154.23.83.67	true	true		unknown
www.firsttimephysics.com	208.91.197.27	true	true		unknown
www.illoftapartments.com	unknown	unknown	true		unknown
www.manno.expert	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.illoftapartments.com/uecu/?2d3pCdLh=I+cFmvzvjfujRN3oltevYzRyUOJqDj5YxiqkJ4i7Zjmur1++tOYpTWGX3hXOvnB+KlCx&fXJ=z64Txz	false	• Avira URL Cloud: safe	unknown
http://www.firsttimephysics.com/uecu/?2d3pCdLh=hr7+JRYyT1HVyDshWD8v/2ivT/o36mEBRVmbpvRN6jTQqfRWnpyet8LANEukLjLgYMOr&fXJ=z64Txz	true	• Avira URL Cloud: safe	unknown
www.illoftapartments.com/uecu/	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	illoftapartments.com	United States		15169	GOOGLEUS	false
208.91.197.27	www.firsttimephysics.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
173.254.28.149	www.dipmarketingagency.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458954
Start date:	03.08.2021
Start time:	22:30:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_Advice.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@11/1@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.8% (good quality ratio 31.9%) • Quality average: 71.7% • 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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.197.27	jnl3kWNWWS.exe	Get hash	malicious	Browse	• www.certifiedlaywernj.com/uoe8/?lN94pX=KQL1U0jkwOK6bk9f0TEfGgpSk6NYazXrF0FfkI9y7fgaIWuwCAJ47CYWlNurQr1Y4rdS&k4b=_hSD
	2GuNlCn0X6.exe	Get hash	malicious	Browse	• www.gmcworktrucksandvans.com/ushb/?5j5=l1O/uck6g9walBnW5BVONfuZZqB0SN9ZqTQRctHuIhSHtr3ojOmVpygYbjT42+AiDZ+z&PjND=Mlr4_4Sx
	Order=bcm_28062021.exe	Get hash	malicious	Browse	• www.researchinnovations.net/uqf5/?R2Jl=vPwqlu4x75djMEhpCHQA4gFf+95PxNUJ1qFGdpB6Q1QDKe6EVaB/Nk3rDLbvZfGP03YT&6lN=JfrLUXyhkZc
	0rder-bcm_23062021.exe	Get hash	malicious	Browse	• www.researchinnovations.net/uqf5/?kRwl=vPwqlu4x75djMEhpCHQA4gFf+95PxNUJ1qFGdpB6Q1QDKe6EVaB/Nk3rDLbvZfGP03YT&5joHs0=8pFHanmpiBY0
	Purchase_Order.exe	Get hash	malicious	Browse	• www.researchinnovations.net/uqf5/?6lU=cB64Yhz&oli=vPwqlu4x75djMEhpCHQA4gFf+95PxNUJ1qFGdpB6Q1QDKe6EVaB/Nk3rDI7VJOm3uQ5U
	CIh8xCD9fi.exe	Get hash	malicious	Browse	• www.rentmystuff.info/sh2m/?o8bHpX=TSNWRgvJWBu1BreqPwc9vl9kVz+0+Hx/d5736XfHbnyatGnwwsv7zfxbAWBBdgyQ/d5H&RFQLz=3fQttPI8YNYDZ
	919780-920390.exe	Get hash	malicious	Browse	• www.wheretheresaytheresaway.com/i3vu/?5j=c4V+ikE91G8kkdotqrW9bbIjBlPXHb2qceIJ/0ViGlJ3NVG8dy1ZG+wt654cEGlfVBc2&j4=SZLXJF7Pq6w8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	03062021.exe	Get hash	malicious	Browse	• www.researchinnovations.net/uqf5/?6lzX=vPwqlu4x75djMEhpCHQA4gFf+95PxNUJ1qFGdpB6Q1QDKe6EVaB/Nk3rDLbvZfGP03YT&EJBD=f0GHX
	wire_confirmation.pdf.exe	Get hash	malicious	Browse	• www.seniorliving100ig.com/m3rc/?2dG4=a/WbhIk1O3pNWs/fl0DnukaPSE5qtuU08n35/l03yzwKMXEJ+D24oHXDPuKusACIaWhK&W8L0b=6l68FPWpppFp
	CONTRACT SWIFT.exe	Get hash	malicious	Browse	• www.rnrsans.com/s5cm/?IBZlYbB=56Wx/iK0XerXx9sRleo+Maj0Gmk9CoRfrFFa5e3vq65qm4nwUyEHtu+AOd1TMQjYkOCiNEfRCw==&7no=4hLljrWPCjYL
	SHIPPING DOCUMENT_7048555233PDF.exe	Get hash	malicious	Browse	• www.rnrsans.com/s5cm/?jrTDmX=56Wx/iK0XerXx9sRleo+Maj0Gmk9CoRfrFFa5e3vq65qm4nwUyEHtu+AOd5TfAvb9eC0&p0G=ndfPKtxxGRrhJ
	PO_2021005.exe	Get hash	malicious	Browse	• www.seniorliving100ig.com/m3rc/?tFQl=XPoLWrCp&kr74WFG=a/WbhIk1O3pNWs/fl0DnukaPSE5qtuU08n35/l03yzwKMXEJ+D24oHXDPuKEzwyIeUpK
	Pdf Scen Invoice 17INV06003.exe	Get hash	malicious	Browse	• www.dfhgear.com/s5cm/?0bMpLRa=5u8mVReR2sf6Zr+bnzJEGrTMXUs6rQplQOF7eIj26SdfoaNehkvQkkmk6FvxoWrQXp5c&k2JxoV=fDKdgJeh5
	MT103 - Remittance.exe	Get hash	malicious	Browse	• www.rnrsans.com/s5cm/?tZkPXV-=56Wx/iK0XerXx9sRleo+Maj0Gmk9CoRfrFFa5e3vq65qm4nwUyEHtu+AOd5TfAvb9eC0&U4ht=Ovpduruh8Z5tNNP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ Catalogues 00645.exe	Get hash	malicious	Browse	• www.blowmei.net/bc9h/?rZyXur=zRPrWGkp8LYfW4P8bcsHO+/BMP9KI+2YDvoaSjg68eXWEE7ZaovsRiIw9IfCCD0rhYCx&Ezr47v=arITk8jHBbY8Nj
	RFQ Catalogues 00934.exe	Get hash	malicious	Browse	• www.blowmei.net/bc9h/?DxoLn=zRPrWGkp8LYfW4P8bcsHO+/BMP9KI+2YDvoaSjg68eXWEE7ZaovsRiIw9LzSeyoQmtrg0oH+xA==&anM=TXFx4Prp_d9P
	PDF Purchase Order #RFQ7787HG00.exe	Get hash	malicious	Browse	• www.rnrsans.com/s5cm/?jJE=56Wx/iK0XerXx9sRleo+Maj0Gmk9CoRfrFFa5e3vq65qm4nwUyEHtu+AOd1qThDbqYelNEfWRA==&wXO=O2Mtwpn
	O1E623TjjW.exe	Get hash	malicious	Browse	• www.certifiedlaywernj.com/uoe8/?hL3=KQL1U0jkwOK6bk9f0TEfGgpSk6NYazXrF0Ffkl9y7fgalWuwCAJ47CYWlNirD75bh7dEhobd5A==&lN68=VTUTzPuXE25p9L
	krJF4BtzSv.exe	Get hash	malicious	Browse	• www.iryna zumba.com/oerg/?YL0=8pN4l4&r6A=xkxlBTP84BDqik+ZtVg23Y9Efr+3g0otXhZL96a2dhmKBXhQvXR65tW6hH0zY1naWy08
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• www.iryna zumba.com/oerg/?ndndnZ=UtWlYrO0rhjH&mHLD_0=xkxlBTP84BDqik+ZtVg23Y9Efr+3g0otXhZL96a2dhmKBXhQvXR65tW6hEUJIkHiMVV7

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	RuVwYj2Jax.exe	Get hash	malicious	Browse	• 192.185.77.139
	KkPVouLuOx.exe	Get hash	malicious	Browse	• 67.20.76.71

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 162.241.218.97
	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 162.241.216.53
	Amaury.vanvinckenroye-AudioMessage_520498.htm	Get hash	malicious	Browse	• 192.185.138.88
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 50.87.146.49
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 74.220.199.6
	hD72Gd3THG.exe	Get hash	malicious	Browse	• 67.20.76.71
	Products Order38899999.exe	Get hash	malicious	Browse	• 50.87.146.199
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	WWTLJo3vxn.exe	Get hash	malicious	Browse	• 192.254.23 5.241
	INV. 736392 Scan pdf.exe	Get hash	malicious	Browse	• 192.185.16 4.148
	7nNtjBvhrm	Get hash	malicious	Browse	• 142.7.147.90
	Purchase Requirements.exe	Get hash	malicious	Browse	• 192.185.0.218
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	• 162.241.217.69
	Products Order.exe	Get hash	malicious	Browse	• 50.87.146.199
	zerYOlEkZR.exe	Get hash	malicious	Browse	• 192.254.23 5.241
	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	• 192.185.90.36
	csa customers.xlsx	Get hash	malicious	Browse	• 162.241.21 7.138
	ENXcmU1LzQ.exe	Get hash	malicious	Browse	• 108.167.158.96
CONFLUENCE-NETWORK-INCVG	INVOICE_0002_PDF.exe	Get hash	malicious	Browse	• 209.99.40.222
	Purchase Requirements.exe	Get hash	malicious	Browse	• 209.99.40.222
	SGKCM20217566748_Federighi Turkiye Oferta Term#U00e9k .exe	Get hash	malicious	Browse	• 208.91.197.39
	PO_0008.exe	Get hash	malicious	Browse	• 209.99.40.222
	QVwfduoULs.exe	Get hash	malicious	Browse	• 209.99.40.222
	csa customers.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	altnp3zI5hfg3Eg.exe	Get hash	malicious	Browse	• 204.11.56.48
	0020072921_Swift_Payment_Details.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• 209.99.40.222
	RFQ# 626669 .xlsx	Get hash	malicious	Browse	• 204.11.56.48
	Nsda7LTM1x.exe	Get hash	malicious	Browse	• 204.11.56.48
	367006.exe	Get hash	malicious	Browse	• 209.99.40.222
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 208.91.197.91
	i2Kzh5TEhc.exe	Get hash	malicious	Browse	• 209.99.40.222
	PURCHASE ORDER 72121.exe	Get hash	malicious	Browse	• 209.99.64.70
	MtYE4LZNQy.exe	Get hash	malicious	Browse	• 204.11.56.48
	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 204.11.56.48
	mal.exe	Get hash	malicious	Browse	• 209.99.64.55
	vjsBNwolo9.js	Get hash	malicious	Browse	• 204.11.56.48

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Payment_Advice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Advice.exe.log	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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..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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.607757014307062
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:	Payment_Advice.exe
File size:	881664
MD5:	b5a3a16559c14a2db6837fb8792134ae
SHA1:	31280391b1a399a3bc1c8ea0f4fb27e2dc9e56a0
SHA256:	c8ff043caee4e9cc889d1b7f8149e5c59ec43d2d01edeb49cb40fe1fd09a233a
SHA512:	c4ab64e5b18825e5f499182855de4ebb937aec980544b9e5accc8c5a8513fe48c3fb3b317b80eff463c32ff2ff8a20825ad196bf22a21281149e14cde3234e89
SSDEEP:	24576:pWF05yIQeYdWmi3xn+3O/Q6l0gtdc/yrWKF9eNNIp:NsdVi3xn2O466gtnfrejIp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..h..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d86d6
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:	0x6101F213 [Thu Jul 29 00:10:59 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

General

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	0xd66dc	0xd6800	False	0.834330383159	COM executable for DOS	7.61652787362	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xda000	0x604	0x800	False	0.3388671875	data	3.43614330066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	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
08/03/21-22:32:59.457711	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	34.102.136.180	192.168.2.3
08/03/21-22:33:04.541323	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	34.102.136.180
08/03/21-22:33:04.541323	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	34.102.136.180
08/03/21-22:33:04.541323	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	34.102.136.180
08/03/21-22:33:04.655507	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49738	34.102.136.180	192.168.2.3
08/03/21-22:33:15.937650	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	154.23.83.67
08/03/21-22:33:15.937650	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	154.23.83.67
08/03/21-22:33:15.937650	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.3	154.23.83.67

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:32:53.375864029 CEST	192.168.2.3	8.8.8.8	0xe0c2	Standard query (0)	www.dipmarketingagency.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:32:59.267330885 CEST	192.168.2.3	8.8.8.8	0xa8f4	Standard query (0)	www.illoftapartments.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:33:04.485091925 CEST	192.168.2.3	8.8.8.8	0x6aaa	Standard query (0)	www.manno.expert	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:09.705560923 CEST	192.168.2.3	8.8.8.8	0xa2d4	Standard query (0)	www.firsttimephysics.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:15.503002882 CEST	192.168.2.3	8.8.8.8	0x2fd2	Standard query (0)	www.quickoprintnv.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:21.547020912 CEST	192.168.2.3	8.8.8.8	0xdb3a	Standard query (0)	www.missabrams.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:32:53.415488005 CEST	8.8.8.8	192.168.2.3	0xe0c2	No error (0)	www.dipmarketingagency.com		173.254.28.149	A (IP address)	IN (0x0001)
Aug 3, 2021 22:32:59.311240911 CEST	8.8.8.8	192.168.2.3	0xa8f4	No error (0)	www.illoftapartments.com	illoftapartments.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:32:59.311240911 CEST	8.8.8.8	192.168.2.3	0xa8f4	No error (0)	illoftapartments.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:04.522651911 CEST	8.8.8.8	192.168.2.3	0x6aaa	No error (0)	www.manno.expert	manno.expert		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:33:04.522651911 CEST	8.8.8.8	192.168.2.3	0x6aaa	No error (0)	manno.expert		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:09.849842072 CEST	8.8.8.8	192.168.2.3	0xa2d4	No error (0)	www.firsttimephysics.com		208.91.197.27	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:15.699641943 CEST	8.8.8.8	192.168.2.3	0x2fd2	No error (0)	www.quickoprintnv.com		154.23.83.67	A (IP address)	IN (0x0001)
Aug 3, 2021 22:33:21.727320910 CEST	8.8.8.8	192.168.2.3	0xdb3a	No error (0)	www.missabrams.com		45.197.108.106	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dipmarketingagency.com
- www.illoftapartments.com
- www.manno.expert
- www.firsttimephysics.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49736	173.254.28.149	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:32:53.592602015 CEST	4482	OUT	GET /uecu/?fXJ=z64Txz&2d3pCdLh=s7j1QsnOxn4iRchbaINLVToxitdCMGa8G3lQ/6LX9JGbR/ScT5dxpPHG5+tB2xnbOyUI HTTP/1.1 Host: www.dipmarketingagency.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:32:54.633936882 CEST	4484	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 03 Aug 2021 20:32:53 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://dipmarketingagency.com/uecu/?fXJ=z64Txz&2d3pCdLh=s7j1QsnOxn4iRchbaINLVToxitdCMGa8G3lQ/6LX9JGbR/ScT5dxpPHG5+tB2xnbOyUI Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:32:59.344643116 CEST	4485	OUT	GET /uecu/?2d3pCdLh=I+cFmvzvjfujRN3oltevYzRyUOJqDj5YxiqkJ4i7Zjmur1++tOYpTWGX3hXOvnB+KlCx&fXJ=z64Txz HTTP/1.1 Host: www.illoftapartments.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:32:59.457710981 CEST	4486	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 20:32:59 GMT Content-Type: text/html Content-Length: 275 ETag: "6104856e-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> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49738	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:33:04.541322947 CEST	4487	OUT	GET /uecu/?fXJ=z64Txz&2d3pCdLh=u60vTBsF9oPaXHkJdoxCc4Kqv5IVcROu1QUUkePEY82yQrKo/wvecAMYDl3vDcEzgvnI HTTP/1.1 Host: www.manno.expert Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:33:04.655507088 CEST	4487	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 20:33:04 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> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49739	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:33:09.989584923 CEST	4488	OUT	GET /uecu/?2d3pCdLh=hr7+JRYyT1HVyDshWD8v/2ivT/o36mEBRVmbpvRN6jTQqfRWnpyet8LANEukLjLgYMOr&fXJ=z64Txz HTTP/1.1 Host: www.firsttimephysics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:33:10.564115047 CEST	4490	IN	HTTP/1.1 200 OK Date: Tue, 03 Aug 2021 20:33:10 GMT Server: Apache Set-Cookie: vsid=928vr3755683901805043; expires=Sun, 02-Aug-2026 20:33:10 GMT; Max-Age=157680000; path=/; domain=www.firsttimephysics.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_UtSH/Dss0NKZhGcIqXH9OJsftz5HWN/7clY2 DINsRw9aSkdX6t12uw/Ci8ieJf9OIyE2jhOASMSdcjGZJ8sWtw== Keep-Alive: timeout=5, max=80 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 61 63 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 6b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 55 74 53 48 2f 44 73 73 30 4e 4b 5a 68 47 63 49 71 58 48 39 4f 4a 73 66 74 7a 35 48 57 4e 2f 37 63 6c 59 32 44 49 4e 73 52 77 39 61 53 6b 64 58 36 74 31 32 75 77 2f 43 69 38 69 65 4a 66 39 4f 49 79 45 32 6a 68 4f 41 53 4d 53 64 63 6a 47 5a 4a 38 73 57 74 77 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 69 72 73 74 74 69 6d 65 70 68 79 73 69 63 73 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 69 72 73 74 74 69 6d 65 70 68 79 73 69 63 73 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d Data Ascii: 4acb<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_UtSH/ Dss0NKZhGcIqXH9OJsftz5HWN/7clY2DINsRw9aSkdX6t12uw/Ci8ieJf9OIyE2jhOASMSdcjGZJ8sWtw==""><head><script t ype="text/javascript">var abp;</script><script type="text/javascript" src="http://www.firsttimephysics.com/px.js?ch=1"> /script><script type="text/javascript" src="http://www.firsttimephysics.com/px.js?ch=2"></script><script type="text/java script">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height=

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Payment_Advice.exe PID: 2648 Parent PID: 5724

General

Start time:	22:31:08
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Payment_Advice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice.exe'
Imagebase:	0xd30000
File size:	881664 bytes
MD5 hash:	B5A3A16559C14A2DB6837FB8792134AE

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: 00000000.00000002.292779519.000000000420A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.292779519.000000000420A000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.292779519.000000000420A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.292646120.0000000004149000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.292646120.0000000004149000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.292646120.0000000004149000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.291281843.00000000031B1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 1156 Parent PID: 2648

General

Start time:	22:31:47
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xe0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5756 Parent PID: 2648

General

Start time:	22:31:48
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 2344 Parent PID: 2648

General

Start time:	22:31:48
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x440000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 0000000C.00000002.355992168.0000000000A80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.355992168.0000000000A80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.355992168.0000000000A80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.356268880.0000000000AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.356268880.0000000000AB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.356268880.0000000000AB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.355215445.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.355215445.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.355215445.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 2344

General

Start time:	22:31:51
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: colorcpl.exe PID: 1156 Parent PID: 3388

General

Start time:	22:32:15
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x2c0000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000015.00000002.470886740.00000000025B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.470886740.00000000025B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.470886740.00000000025B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.469653459.0000000000470000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.469653459.0000000000470000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.469653459.0000000000470000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2288 Parent PID: 1156

General

Start time:	22:32:20
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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: 4000 Parent PID: 2288

General

Start time:	22:32:21
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