ID: 483527
Sample Name: Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe
Cookbook: default.jbs
Time: 08:14:45
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

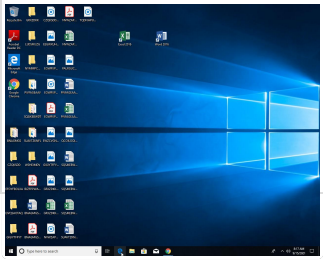
Windows Analysis Report Electronic Payment Remittan…

Overview

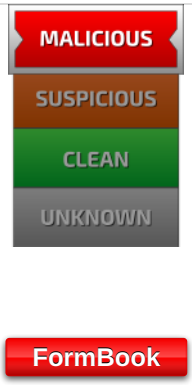
General Information

Sample Name:	Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe
Analysis ID:	483527
MD5:	e29285288905eb..
SHA1:	3c656f9257b7630.
SHA256:	7027a232f8327a5.
Infos:	

Most interesting Screenshot:



Detection



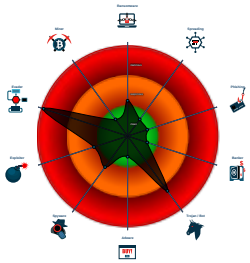
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- 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…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe (PID: 3176 cmdline: 'C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe' MD5: E29285288905EBB27D9E4443BCAA6638)
  - Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe (PID: 4180 cmdline: C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe MD5: E29285288905EBB27D9E4443BCAA6638)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 1392 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - raserver.exe (PID: 3652 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 912 cmdline: /c del 'C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.fasilitatortoefl.com/uytf/"
  ],
  "decoy": [
    "estherestates.online",
    "babyballetwigan.com",
    "ignorantrough.xyz",
    "moominmamalog.com",
    "pasticcerialemmi.com",
    "orangstyle.com",
    "oldwaterfordfarm.com",
    "aiiqiuwnsas.com",
    "youindependents.com",
    "runbank.net",
    "phytolipshine.com",
    "almedmedicalcenter.com",
    "czxzsa.com",
    "yummyblockparty.com",
    "gadgetinfo.info",
    "cloudfolderplayer.com",
    "chowding.com",
    "xn--tarzmbu-ufb.com",
    "danielaasab.com",
    "dreampropertiesluxury.com",
    "itsready.support",
    "freepoeople.com",
    "richesosity.online",
    "covidbrainfogsyndrome.com",
    "hide.osaka",
    "fitotec.net",
    "cdfdwj.com",
    "vjr.realestate",
    "knowit.today",
    "sellhomefastinorlando.com",
    "permacademy.net",
    "andhraadvocates.com",
    "rochainrevsry.xyz",
    "casino-virtuali.net",
    "liptondesignstudio.xyz",
    "keyinternationals.com",
    "gamifibase.com",
    "atjehtimur.com",
    "hobonickelsvillarrubia.com",
    "johnharrisagent.com",
    "preabsorb.xyz",
    "likevietsub38.com",
    "getrichandsavetheworld.com",
    "livelife2dance.com",
    "juesparza.com",
    "buffalocreekdesign.com",
    "diegos.xyz",
    "covidforensicaudit.com",
    "popitperu.com",
    "gczvahqeg.site",
    "aspireship.tech",
    "freedomforfarmedrabbits.online",
    "pasalsacongress.com",
    "custommetalimagery.photography",
    "managementcoachinginc.com",
    "hxysjkj.com",
    "trusticoin.biz",
    "wireconnectaz.tech",
    "yoiseikatsu.net",
    "slggroups.com",
    "curiousmug.com",
    "svetarielt.site",
    "nongormart.com",
    "btt5204.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.302114370.00000000012D0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.302114370.00000000012D0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.302114370.00000000012D0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000013.00000002.474783464.0000000000AF0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.474783464.0000000000AF0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
5.2.Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

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

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

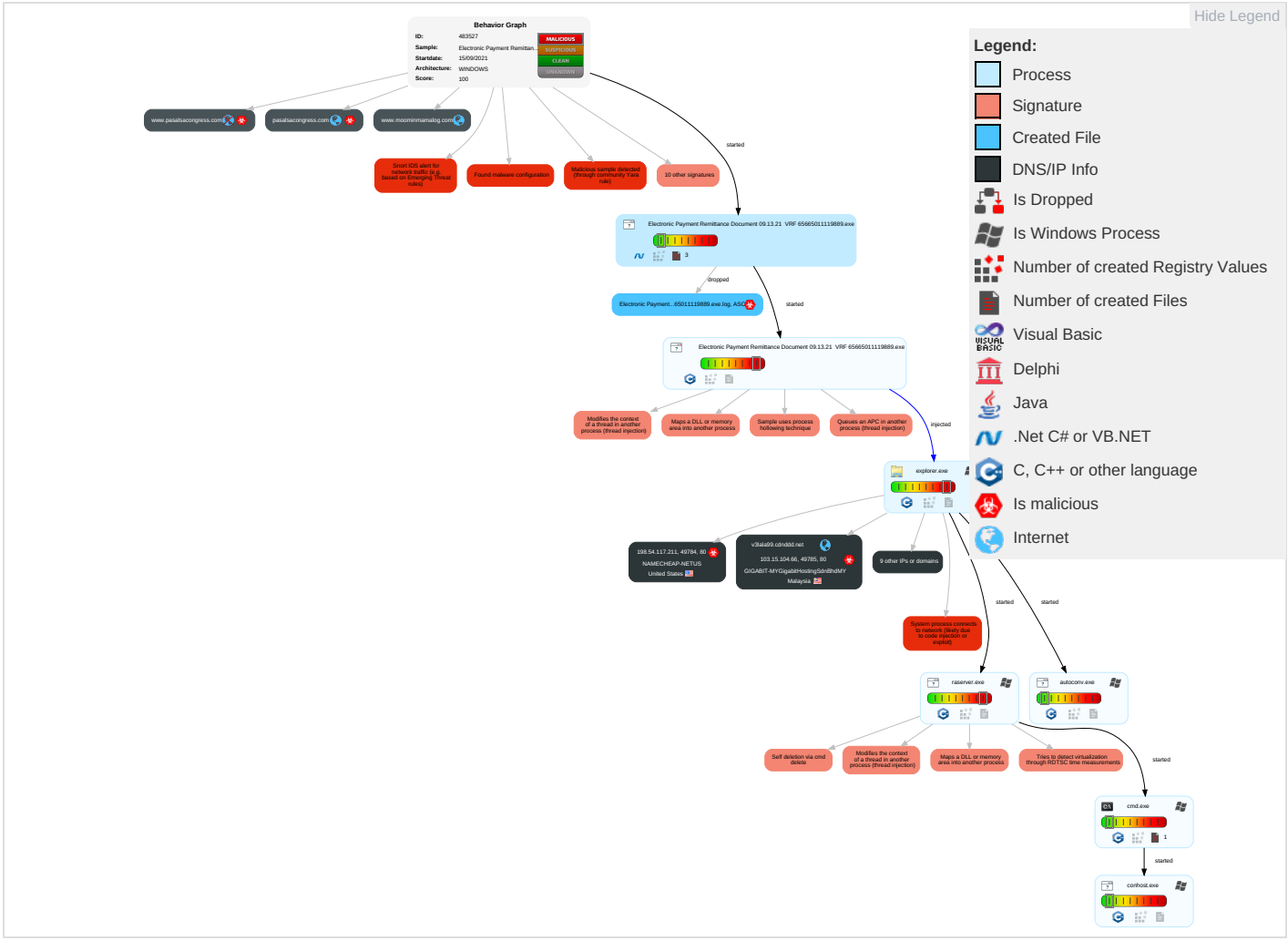
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Pho 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 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	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 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
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 t 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
Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe	28%	Virustotal		Browse
Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/HO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritaHO	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ty	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.goodfont.co.krKKd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.fontbureau.com-O6d	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttod	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/eOndo	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comasF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/0O	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr2K	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/lOyd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/lOyd	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnly	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
www.fasilitatortoefl.com/uytf/	0%	Avira URL Cloud	safe	
http://www.carterandcone.com9	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFsO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv	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.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/It	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritolOyd	0%	Avira URL Cloud	safe	
http://www.btt5204.com/uytf/?4hax=0R01lDMz+xXIWoinSyO5qQyNMJHeVacFioz47MHPNe7DMd9wx+TtySfTu0uIVXra7tyR&6lE=xT6Pc	0%	Avira URL Cloud	safe	
http://www.itsready.support/uytf/?4hax=Lw8pQUl/qe2gQHW8JEklnfX9vlL4ErZAhlphDfsrttl8uYXfrtRE5waSCzthMEOsFHNR&6lE=xT6Pc	0%	Avira URL Cloud	safe	
http://www.fontbureau.comS	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceva	0%	Avira URL Cloud	safe	
http://www.carterandcone.comYou	0%	Avira URL Cloud	safe	
http://www.carterandcone.como	0%	URL Reputation	safe	
http://www.founder.com.cn/cncz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0nl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krQK	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comdAO	0%	Avira URL Cloud	safe	
http://www.carterandcone.com%$l/d	0%	Avira URL Cloud	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.como..	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.carterandcone.comz	0%	Avira URL Cloud	safe	
http://www.carterandcone.comy	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;O$dh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.micro(D.df	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnrsCI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/VO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/0O	0%	Avira URL Cloud	safe	
http://www.carterandcone.comueh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-O6d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pasalsacongress.com	192.185.52.175	true	true		unknown
parkingpage.namecheap.com	198.54.117.215	true	false		high
www.johnharrisagent.com	52.71.133.130	true	false		high
v3lala99.cdnddd.net	103.15.104.66	true	true		unknown
www.moominmamalog.com	183.181.96.104	true	false		unknown
www.yummyblockparty.com	unknown	unknown	true		unknown
www.hide.osaka	unknown	unknown	true		unknown
www.pasalsacongress.com	unknown	unknown	true		unknown
www.fitotec.net	unknown	unknown	true		unknown
www.btt5204.com	unknown	unknown	true		unknown
www.itsready.support	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.fasilitatortoefl.com/uytf/	true	• Avira URL Cloud: safe	low
http://www.btt5204.com/uytf/?4hax=0R01lDMz+xXIWoinSyO5qQyNMJHeVacFioz47MHPNe7DMd9wx+TtySfTu0uIVXra7tyR&6lE=xT6Pc	true	• Avira URL Cloud: safe	unknown
http://www.itsready.support/uytf/?4hax=Lw8pQUl/qe2gQHW8JEklnfX9vIL4ErZAhlphDfsrttl8uYXfrtRE5waSCzthMEOsFHNR&6lE=xT6Pc	true	• Avira URL Cloud: safe	unknown
http://www.johnharrisagent.com/uytf/?4hax=1GgOydTR9rFB1tFiaPZsKtEWQf/ik/nrf61jzTsng/4mIf33LxMFmIGp7DtpN0+eCTBT&6lE=xT6Pc	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.71.133.130	www.johnharrisagent.com	United States		14618	AMAZON-AESUS	false
198.54.117.211	unknown	United States		22612	NAMECHEAP-NETUS	true
103.15.104.66	v3lala99.cdnddd.net	Malaysia		55720	GIGABIT-MYGigabitHostingSdnBhdMY	true
198.54.117.215	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483527
Start date:	15.09.2021
Start time:	08:14:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.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:	28
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@8/1@11/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.9% (good quality ratio 57.1%) • Quality average: 69.4% • Quality standard deviation: 32.7%
HCA Information:	• Successful, ratio: 97% • 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
08:15:36	API Interceptor	64x Sleep call for process: Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.71.133.130	catalogo campione_0021.exe	Get hash	malicious	Browse	• www.blonohomesales.com/p3q8/?XjEP7rn=SmJymXHTOHzh2mODpH0/b6a2rttU4EqyY620WTN4/2YO0WOF3CKHJjBQQ+H+msZQkWXKyJfovg==&QPK=5jV4hVZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	revised quotation.exe	Get hash	malicious	Browse	• www.britr obertsreal tor.com/n58i/?MDHhFT=mBK5C8kKNeLnOBRL/3T2hMZE7okfl7IAcP/kfUwDuOFDQo447qX7+h6WtHNcYYtcMFZ+&h6=u0DLr058
	NEW ORDER.exe	Get hash	malicious	Browse	• www.britr obertsreal tor.com/n58i/?0FNpaj8=mBK5C8kKNeLnOBRL/3T2hMZE7okfl7IAcP/kfUwDuOFDQo447qX7+h6WtHN2HodcIHR+&rPJpgz=GBMHuTwhVBI
	BL COPY.exe	Get hash	malicious	Browse	• www.britr obertsreal tor.com/n58i/?tr4x8=1bxhLR18&IX3h5l=mBK5C8kKNeLnOBRL/3T2hMZE7okfl7IAcP/kfUwDuOFDQo447qX7+h6WtHNcYYtcMFZ+
	bH8nV98LYu.exe	Get hash	malicious	Browse	• www.shirl eyabrowerr ealtor.com/fa0p/?zR0XgB=gPIx3pDxYlK&4hl0ibR=MvRmTuLwwyQZwgK3YYiG7KB5GvnBlUZ8DFUO14mvl6WqMsSM4hixWFgVlLnCQryC99za
	xrHGQS1rz2.exe	Get hash	malicious	Browse	• www.irene higginson. com/i7dg/?Qz=KBZ4dj0XENkP&2dnpGhRp=RKv9R3r324rqECNMQpwQcD+TtNzrebiuQaqq6euW1C9OfeVYpIPiEjipJWSoTYE6epD/
	Scan#0068-46c3365.exe	Get hash	malicious	Browse	• www.andre wsteelsell s.com/q3t0/?-Zl=6idTJ3MAhmjthBNVTJ2XuDMtfLW/2CXP3uLaEMGhGmhlqOq2RVzpVswBfbFOtMAa4qr0&gJBT-f=IFNTv2l8I

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Documents.exe	Get hash	malicious	Browse	• www.hopematthewsrealtor.com/amb6/?c8n=8pm2sjSgmmTSFscavwD5UpILjrVjpPh3mP/S3l2xoyuhTXjCVVPg3vinZEFiQZEl0/31&Vt=QZbpwDmh5dWDM
	IMAGE00037.exe	Get hash	malicious	Browse	• www.jasoneganrealtor.com/kkt/?0DKlKl=cc/nqGYAQYIM3Pt1Xwy2u5TuLJzmwQtvr0clQyawalrzoTK8+eLnoTutccqTHVKswWI+&UL=0balqH
	FASMW.EXE	Get hash	malicious	Browse	• www.findthematchmakerrealtor.com/cabq/?h6R8xP=L/FIdmi9M2kSKwf8ScI+8YDyUdwD7p7Kj2yVOc9WwOzkqPyEJC2VW+A/3pD6I5dSpBvh&iZ=2di86hvH
	EJIMS.exe	Get hash	malicious	Browse	• www.howdysellshomes.com/eo5u/?3fqHGn=ZInpMphxFT&ATRPZLx=yfSEZOF/V+aHR3Qqu+TOTlJolf6SRhlBlkgMTnrUi9a7ISsQSkzVdaPaAGQDw9tGN+zc
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• www.blakehaleyrealestate.com/uwec/?Rl4=YVFTx4yh&GFQl9jnp=9RHT2DLP46lJWlpPTosGw7NRwYJtTk68eEdvTXInG9v5n7yAqhkX2tGT0EYgCY2WM8rv
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• www.blakehaleyrealestate.com/uwec/?v2=9RHT2DLP46lJWlpPTosGw7NRwYJtTk68eEdvTXInG9v5n7yAqhkX2tGT0EYgCY2WM8rv&CZ6=7nExZbW

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• www.blakehaleyrealestate.com/uwec/?-ZVd=1bgta&T8VxaVs=9RHT2DLP46IJWlpPTosGw7NRwYJtTk68eEdvTXInG9v5n7yAqhkX2tGT0EYgCY2WM8rv
	igPVY6UByl.exe	Get hash	malicious	Browse	• www.gregismyrealestateagent.com/evpn/?6lB4ir3X=UDxzuRprqZDJvJoKVzbwL1i6nUgviHPd/6Kvoeyj55HiZxQYyGLzJE1yAaeHFu5gVc5c&lZQ=fxoxjP38
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.melekhemfuzaylovrealtor.com/rrrq/?ATxdA4s=pwrgH0dcWtE6RcnjvsF+gBwj2enFa+fTozhnxLgTWRaQ9ETFCh2EIcQryx3dD2YPpuUAmv+cig==&4hO=uDHPhJlxONuPbDb
	purchase order#034.exe	Get hash	malicious	Browse	• www.patticrumprealestate.com/8ufh/?EzrthRhp=U8w9/jPqiyF9T6rAv+nd1qZLEbDwevisuc0vxVqKX7gCld07x/wriiT59VLN/LUTeuQy&ojo0f=SzrhU8
	dwg.exe	Get hash	malicious	Browse	• www.evamichelleverm eeschrealtor.com/ripw/?YL0=AbZvoGEXXQ2UeGMkjKvPTH9y6CbrSsxy+uP80hsvy1agLthBgMYihPZc0BWoiy3movbA&DhAH08=9rzdODV81V
	PO#416421.exe	Get hash	malicious	Browse	• www.propertiesbyjose.com/wpsb/?GFQL6=9rzdF4d0LhP&pvbxILHp=HEs1UZJZzTZh4b/CLgTQtUFl/p4LqgX1DDiD2qBPcXJWn7sMmrEWnzV34lgPleSeyaCceIjMPg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	POgMmI.exe	Get hash	malicious	Browse	• www.landeverrealestate.com/wsu/?FDHH=o0d7uZds/Uq3OyNWot+oiPxVX9Lhq1LOweo6JSl71P7OyksdMpdvphbquE+Kn7tuvWRF0Atuwg==&Rl=Vtx0J

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	debit.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	Data Sheet and Profile.exe	Get hash	malicious	Browse	• 198.54.117.215
	4444.exe	Get hash	malicious	Browse	• 198.54.117.218
	3RBawvxxeY.exe	Get hash	malicious	Browse	• 198.54.117.210
	grace $$.exe	Get hash	malicious	Browse	• 198.54.117.212
	RFQ_PO_009890_pdf.exe	Get hash	malicious	Browse	• 198.54.117.210
	SpZP2QerMU.exe	Get hash	malicious	Browse	• 198.54.117.211
	Purchase Order# 210145.exe	Get hash	malicious	Browse	• 198.54.117.215
	RFQ 10305 .xlsx	Get hash	malicious	Browse	• 198.54.117.212
	BIN.exe	Get hash	malicious	Browse	• 198.54.117.216
	REMMITANCE COPY.exe	Get hash	malicious	Browse	• 198.54.117.210
	jxotfrv2bv.exe	Get hash	malicious	Browse	• 198.54.117.212
	zXv0Gd4tPi.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO747484992.exe	Get hash	malicious	Browse	• 198.54.117.217
	YgAynTdpcncdnG4.exe	Get hash	malicious	Browse	• 198.54.117.217
	PO_PRICE_REQUEST_00989_PDF.exe	Get hash	malicious	Browse	• 198.54.117.212
	New order.pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	PO.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	Transfer_form_$157,890.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	GosMzUpnGu.exe	Get hash	malicious	Browse	• 198.54.117.217

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	PO7420.exe	Get hash	malicious	Browse	• 52.4.209.250
	DLH1TwLBhW.exe	Get hash	malicious	Browse	• 50.16.244.183
	avxeC9Wssi	Get hash	malicious	Browse	• 54.57.110.152
	Quotation urgent.exe	Get hash	malicious	Browse	• 52.201.24.227
	KOC RFQ.doc	Get hash	malicious	Browse	• 52.204.77.43
	PO. 2100002_pdf_____.exe	Get hash	malicious	Browse	• 3.223.115.185
	hhh.mp3.dll	Get hash	malicious	Browse	• 54.243.45.255
	xrm4z50ja9.exe	Get hash	malicious	Browse	• 54.83.52.76
	Swift Trf.exe	Get hash	malicious	Browse	• 52.201.24.227
	HjlXsbs4Jg	Get hash	malicious	Browse	• 54.142.124.216
	7b388AC1Fw	Get hash	malicious	Browse	• 44.194.145.151
	DPD.apk	Get hash	malicious	Browse	• 50.16.244.183
	Po2142021.xlsx	Get hash	malicious	Browse	• 18.213.250.117
	FlashPlayerUpdate.apk	Get hash	malicious	Browse	• 23.21.76.7
	QcXQmNSaSp	Get hash	malicious	Browse	• 18.207.108.88
	i586	Get hash	malicious	Browse	• 34.231.175.5
	arm	Get hash	malicious	Browse	• 54.133.131.54
	zoD4YzpMMG	Get hash	malicious	Browse	• 54.80.227.212
	mips	Get hash	malicious	Browse	• 34.225.41.128
	x86_64	Get hash	malicious	Browse	• 54.167.122.15
GIGABIT-MYGigabitHostingSdnBhdMY	Clh974QBqG	Get hash	malicious	Browse	• 103.21.89.29
	k6uiZJTzLi.exe	Get hash	malicious	Browse	• 103.91.67.83
	Y22uvB2lnU.exe	Get hash	malicious	Browse	• 103.91.67.83
	sbFQSOHQS9.exe	Get hash	malicious	Browse	• 43.231.4.7
	zidwvnFsej.exe	Get hash	malicious	Browse	• 43.231.4.7
	awVwuEPo4t.exe	Get hash	malicious	Browse	• 43.231.4.7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jr8m2SSa1e.exe	Get hash	malicious	Browse	• 43.231.4.7
	z33RH5liBO.exe	Get hash	malicious	Browse	• 103.91.67.83
	OIHcOp52HF.exe	Get hash	malicious	Browse	• 43.231.4.7
	n5MFenscid.exe	Get hash	malicious	Browse	• 43.231.4.7
	v6TB5C7KtW.exe	Get hash	malicious	Browse	• 43.231.4.7
	OhfbJIz1X7.exe	Get hash	malicious	Browse	• 43.231.4.7
	02xCEgwyK3.exe	Get hash	malicious	Browse	• 43.231.4.7
	refno.exe	Get hash	malicious	Browse	• 103.91.67.83
	oaG6jOntjL	Get hash	malicious	Browse	• 103.229.227.24
	UZOM POWER.exe	Get hash	malicious	Browse	• 103.27.74.97
	JFBlvEr5H9.exe	Get hash	malicious	Browse	• 103.91.67.83
	olG7GnXKKT.exe	Get hash	malicious	Browse	• 103.91.67.83
	ORDER 200VPS.xlsx	Get hash	malicious	Browse	• 103.91.67.83
	uLTvM5APNY.exe	Get hash	malicious	Browse	• 43.231.4.7
NAMECHEAP-NETUS	P67mzce6yI.exe	Get hash	malicious	Browse	• 198.54.122.60
	Gu#U00eda de carga.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	debit.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	Pharmaceutical Inquiry.doc	Get hash	malicious	Browse	• 198.54.122.60
	diagram-129.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-129.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-129.doc	Get hash	malicious	Browse	• 198.54.124.27
	deck.exe	Get hash	malicious	Browse	• 198.54.122.60
	diagram-477.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-477.doc	Get hash	malicious	Browse	• 198.54.124.27
	diagram-477.doc	Get hash	malicious	Browse	• 198.54.124.27
	PO0140092021.doc	Get hash	malicious	Browse	• 198.54.122.60
	I210820-0002 D1#U96a8#U6a5f-#U6d77#U95dc#U767c#U7968-R1_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• 104.219.248.49
	doc03633420210907151503.doc	Get hash	malicious	Browse	• 198.54.122.60
	obizx.exe	Get hash	malicious	Browse	• 104.219.248.49
	fytfireuiwfgdcukyd.doc	Get hash	malicious	Browse	• 198.54.122.60
	DHL-AWD6909800855.doc	Get hash	malicious	Browse	• 104.219.248.49
	wuH92YGkZk.exe	Get hash	malicious	Browse	• 104.219.248.45
	3VFWIsGexy.exe	Get hash	malicious	Browse	• 198.54.115.195

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.log	
Process:	C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x84j:MIHK5HKXE1qHbHK5AHKzvRYHKhQnoPtW
MD5:	E2C3A19FF3EBB1649BF9F41DFE3B7E8F
SHA1:	5DA8AB9561D3C096BB9103413F64EE6E50D5AD88
SHA-256:	18E921771341555EF6167DEBBD7C83727518897E9B4B3545B7CCDB48E2043B74
SHA-512:	6B62A68EC358699D55E4CCD0BBDD4ADDC0F38641D82A019697893CEB503E853A5F087FAF9F4408425AD6631C9CBA31C3354FD98B45F051F2F59A0ECC3CA2FA6
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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\assem

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.463479204604476
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe
File size:	509952
MD5:	e29285288905ebb27d9e4443bcaa6638
SHA1:	3c656f9257b7630e47f57d1326bceafb7481ab29
SHA256:	7027a232f8327a532a1b37586cd42ea73ea0b9c37b1b22334484888f0b13b6b6
SHA512:	16fc6b4d5f0f258ac3887295843553e524276ce4fa127ce01cd49118b8765823885065daf3c2cab716529c6fbe97e2ea47233e88215852b528be6e68e801da1f
SSDEEP:	12288:tqk4DbF53e0IUFLe8OsbVPIBNpvv5Cq9HS2W3wI7GJFY:Gy8dPOX5CSy2WW8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#@a.....0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47daca
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:	0x61402397 [Tue Sep 14 04:22:47 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	0x7bad8	0x7bc00	False	0.845947758838	data	7.48050578829	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x62c	0x800	False	0.34912109375	data	3.50217220911	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	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
09/15/21-08:17:15.112241	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49784	80	192.168.2.3	198.54.117.211
09/15/21-08:17:15.112241	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49784	80	192.168.2.3	198.54.117.211
09/15/21-08:17:15.112241	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49784	80	192.168.2.3	198.54.117.211
09/15/21-08:17:27.003769	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
09/15/21-08:17:36.721776	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
09/15/21-08:17:37.722537	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 08:16:58.536778927 CEST	192.168.2.3	8.8.8.8	0x4b46	Standard query (0)	www.yummyblockparty.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:03.958511114 CEST	192.168.2.3	8.8.8.8	0xb05b	Standard query (0)	www.johnharrisagent.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:09.819931030 CEST	192.168.2.3	8.8.8.8	0x6145	Standard query (0)	www.fitotec.net	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.904324055 CEST	192.168.2.3	8.8.8.8	0xdd0e	Standard query (0)	www.itsready.support	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:25.341937065 CEST	192.168.2.3	8.8.8.8	0x3b69	Standard query (0)	www.btt5204.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:26.330404043 CEST	192.168.2.3	8.8.8.8	0x3b69	Standard query (0)	www.btt5204.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 08:17:32.567346096 CEST	192.168.2.3	8.8.8.8	0x2a90	Standard query (0)	www.hide.osaka	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:33.596535921 CEST	192.168.2.3	8.8.8.8	0x2a90	Standard query (0)	www.hide.osaka	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:34.596653938 CEST	192.168.2.3	8.8.8.8	0x2a90	Standard query (0)	www.hide.osaka	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:40.708005905 CEST	192.168.2.3	8.8.8.8	0x4a8f	Standard query (0)	www.pasalsacongress.com	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:46.537237883 CEST	192.168.2.3	8.8.8.8	0x6f7d	Standard query (0)	www.moominmamalog.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	www.yummyblockparty.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Sep 15, 2021 08:16:58.576446056 CEST	8.8.8.8	192.168.2.3	0x4b46	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:04.009198904 CEST	8.8.8.8	192.168.2.3	0xb05b	No error (0)	www.johnharrisagent.com		52.71.133.130	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:09.867863894 CEST	8.8.8.8	192.168.2.3	0x6145	Name error (3)	www.fitotec.net	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	www.itsready.support	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:14.937865019 CEST	8.8.8.8	192.168.2.3	0xdd0e	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:26.722035885 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	www.btt5204.com	a3m1.cnamek.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:26.722035885 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	a3m1.cnamek.com	izgr3bagus.cdnddd.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:26.722035885 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	izgr3bagus.cdnddd.net	v3lala99.cdnddd.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 08:17:26.722035885 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	v3lala99.cdnddd.net		103.15.104.66	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:27.003680944 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	www.btt5204.com	a3m1.cnamek.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:27.003680944 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	a3m1.cnamek.com	izgr3bagus.cdnddd.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:27.003680944 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	izgr3bagus.cdnddd.net	v3lala99.cdnddd.net		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:27.003680944 CEST	8.8.8.8	192.168.2.3	0x3b69	No error (0)	v3lala99.cdnddd.net		103.15.104.66	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:35.691082954 CEST	8.8.8.8	192.168.2.3	0x2a90	Server failure (2)	www.hide.osaka	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:36.721256018 CEST	8.8.8.8	192.168.2.3	0x2a90	Server failure (2)	www.hide.osaka	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:37.722446918 CEST	8.8.8.8	192.168.2.3	0x2a90	Server failure (2)	www.hide.osaka	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:40.861347914 CEST	8.8.8.8	192.168.2.3	0x4a8f	No error (0)	www.pasalsacongress.com	pasalsacongress.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 08:17:40.861347914 CEST	8.8.8.8	192.168.2.3	0x4a8f	No error (0)	pasalsacongress.com		192.185.52.175	A (IP address)	IN (0x0001)
Sep 15, 2021 08:17:46.814873934 CEST	8.8.8.8	192.168.2.3	0x6f7d	No error (0)	www.moominmamalog.com		183.181.96.104	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.yummyblockparty.com
- www.johnharrisagent.com
- www.itsready.support
- www.btt5204.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49778	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:16:58.763638973 CEST	5871	OUT	GET /uytf/?4hax=Z6tv0ZGri8uWurB8AUDeWgq8Hn78EURDlDEEMIHUNMQGUG9NVGnXX5+ZYyjQXpOA0JMU&6lE=xT6Pc HTTP/1.1 Host: www.yummyblockparty.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
1	192.168.2.3	49779	52.71.133.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:17:04.150310040 CEST	5872	OUT	GET /uytf/?4hax=1GgOydTR9rFB1tFiaPZsKtEWQf/ik/nrf61jzTsng/4mlf33LxMFmIGp7DtpN0+eCTBT&6lE=xT6Pc HTTP/1.1 Host: www.johnharrisagent.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:17:04.289372921 CEST	5873	IN	HTTP/1.1 301 Moved Permanently Server: openresty/1.17.8.2 Date: Wed, 15 Sep 2021 06:17:04 GMT Content-Type: text/html Content-Length: 175 Connection: close Location: https://www.johnharrisagent.com/uytf/?4hax=1GgOydTR9rFB1tFiaPZsKtEWQf/ik/nrf61jzTsng/4mIf3 3LxMFmIGp7DtpN0+eCTBT&6lE=xT6Pc Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 37 2e 38 2e 32 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> openresty/1.17.8.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49784	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:17:15.112241030 CEST	5895	OUT	GET /uytf/?4hax=Lw8pQUl/qe2gQHW8JEklnfX9vlL4ErZAhlphDfsrttl8uYXfrtRE5waSCzthMEOsFHNR&6lE=xT6Pc HTTP/ 1.1 Host: www.itsready.support Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49785	103.15.104.66	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 08:17:27.279082060 CEST	5896	OUT	GET /uytf/?4hax=0R01lDMz+xXIWoinSyO5qQyNMJHeVacFioz47MHPNe7DMd9wx+TtySfTu0uIVXra7tyR&6lE=xT6Pc HTTP/1.1 Host: www.btt5204.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 08:17:27.555051088 CEST	5897	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 15 Sep 2021 06:17:27 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.btt5204.com/uytf/?4hax=0R01lDMz+xXIWoinSyO5qQyNMJHeVacFioz47MHPNe7DMd9wx+TtySf Tu0uIVXra7tyR&6lE=xT6Pc Strict-Transport-Security: max-age=31536000; includeSubDomains Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe PID: 3176 Parent PID: 5236

General

Start time:	08:15:35
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 6566 5011119889.exe'
Imagebase:	0x3c0000
File size:	509952 bytes
MD5 hash:	E29285288905EBB27D9E4443BCAA6638
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.226787168.0000000003841000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.226787168.0000000003841000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.226787168.0000000003841000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.226477640.0000000002862000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe PID: 4180 Parent PID: 3176

General

Start time:	08:15:43
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665 011119889.exe
Imagebase:	0x8a0000
File size:	509952 bytes
MD5 hash:	E29285288905EBB27D9E4443BCAA6638
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: 00000005.00000002.302114370.00000000012D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.302114370.00000000012D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.302114370.00000000012D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.302217110.0000000001300000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.302217110.0000000001300000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.302217110.0000000001300000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.301308375.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.301308375.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.301308375.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 4180

General

Start time:	08:15:45
Start date:	15/09/2021
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
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.255057512.000000000E28B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.255057512.000000000E28B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.255057512.000000000E28B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.271535377.000000000E28B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.271535377.000000000E28B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.271535377.000000000E28B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autoconv.exe PID: 1392 Parent PID: 3388

General

Start time:	08:16:16
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x950000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: raserver.exe PID: 3652 Parent PID: 3388

General

Start time:	08:16:16
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0xc30000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 00000013.00000002.474783464.0000000000AF0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.474783464.0000000000AF0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.474783464.0000000000AF0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.477256169.00000000043F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.477256169.00000000043F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.477256169.00000000043F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.473607935.0000000000700000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.473607935.0000000000700000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.473607935.0000000000700000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 912 Parent PID: 3652

General

Start time:	08:16:20
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Electronic Payment Remittance Document 09.13.21 VRF 65665011119889.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: 1392 Parent PID: 912

General

Start time:	08:16:21
Start date:	15/09/2021
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