ID: 411852
Sample Name:
Inquiry_10_05_2021,pdf.exe
Cookbook: default.jbs
Time: 07:48:43
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

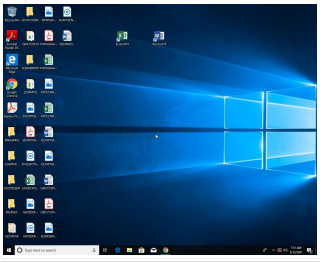
Analysis Report Inquiry_10_05_2021,pdf.exe

Overview

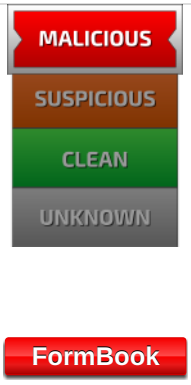
General Information

Sample Name:	Inquiry_10_05_2021,pdf.exe
Analysis ID:	411852
MD5:	d394a8c0a37bcd..
SHA1:	52d386445e5060..
SHA256:	3f4dc309be69548.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

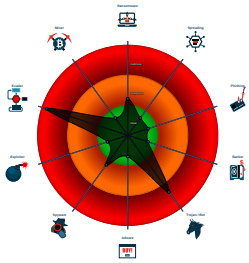


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- Inquiry_10_05_2021,pdf.exe (PID: 1560 cmdline: 'C:\Users\user\Desktop\Inquiry_10_05_2021,pdf.exe' MD5: D394A8C0A37BCDAF432B2882714C6EBA)
  - Inquiry_10_05_2021,pdf.exe (PID: 576 cmdline: C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe MD5: D394A8C0A37BCDAF432B2882714C6EBA)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 2156 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
    - cmmon32.exe (PID: 4772 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
      - cmd.exe (PID: 5068 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 3776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.werealestatephotography.com/hw6d/"
  ],
  "decoy": [
    "medicare101now.com",
    "danahillathletics.com",
    "realjobexpert.com",
    "boulderhalle-hamburg.com",
    "idoweddinghair.com",
    "awdcompanies.com",
    "thevillaflora.com",
    "neutrasystems.com",
    "allwest-originals.com",
    "designtehengsg.com",
    "thenewyorker.computer",
    "ladybugtubs.com",
    "silina-beauty24.com",
    "mifangtu.com",
    "fashionbranddeveloper.com",
    "istanbulhookah.com",
    "askyoyo.com",
    "osaka-computer.net",
    "conegenie.com",
    "agteless.com",
    "carsoncredittx.com",
    "wellalytics.com",
    "onjulitrading.com",
    "thelocallawnmen.com",
    "loanascustomboutique.com",
    "ohcaftanmycaftan.com",
    "ardor-fitness.com",
    "benzinhayvancilik.com",
    "apthaiproperty.com",
    "maxim.technology",
    "dfch18.com",
    "davaoaffordablecondo.com",
    "sueshemp.com",
    "missmaltese.com",
    "lakecountrydems.com",
    "lastminuteminister.com",
    "sofiascelebrations.com",
    "socialaspecthouston.com",
    "rechnung.pro",
    "kathyscrabhouse.com",
    "themusasoficial.com",
    "reversemortgageloanmiami.com",
    "vrventurebsp.com",
    "whatalode.com",
    "xh03.net",
    "qiqihao.site",
    "specstrii.com",
    "organicfarmteam.com",
    "codebinnovations.net",
    "kizunaservice.com",
    "lboclkchain.com",
    "frorool.com",
    "dpok.network",
    "desafogados.com",
    "vestblue.net",
    "forguyshere.com",
    "recordprosperity.info",
    "theballoonbirds.com",
    "adityabirla-loan.com",
    "midgex.info",
    "qishuxia.com",
    "panopticop.com",
    "gd-kangda.com",
    "hotelbrainclub.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.329149948.0000000003A30000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.329149948.0000000003A30000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x29758:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x29ae2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x357f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x352e1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x358f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x35a6f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2a4fa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3455c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2b272:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x3a8e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x3b98a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.329149948.0000000003A30000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x37819:$sqlite3step: 68 34 1C 7B E1 • 0x3792c:$sqlite3step: 68 34 1C 7B E1 • 0x37848:$sqlite3text: 68 38 2A 90 C5 • 0x3796d:$sqlite3text: 68 38 2A 90 C5 • 0x3785b:$sqlite3blob: 68 53 D8 7F 8C • 0x37983:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.463820601.00000000034E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.463820601.00000000034E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

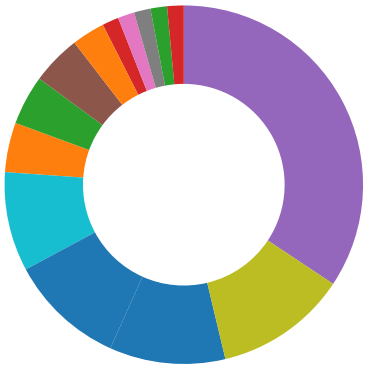
Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.Inquiry_10_05_2021,pdf.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
13.2.Inquiry_10_05_2021,pdf.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
13.2.Inquiry_10_05_2021,pdf.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
13.2.Inquiry_10_05_2021,pdf.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
13.2.Inquiry_10_05_2021,pdf.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$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



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

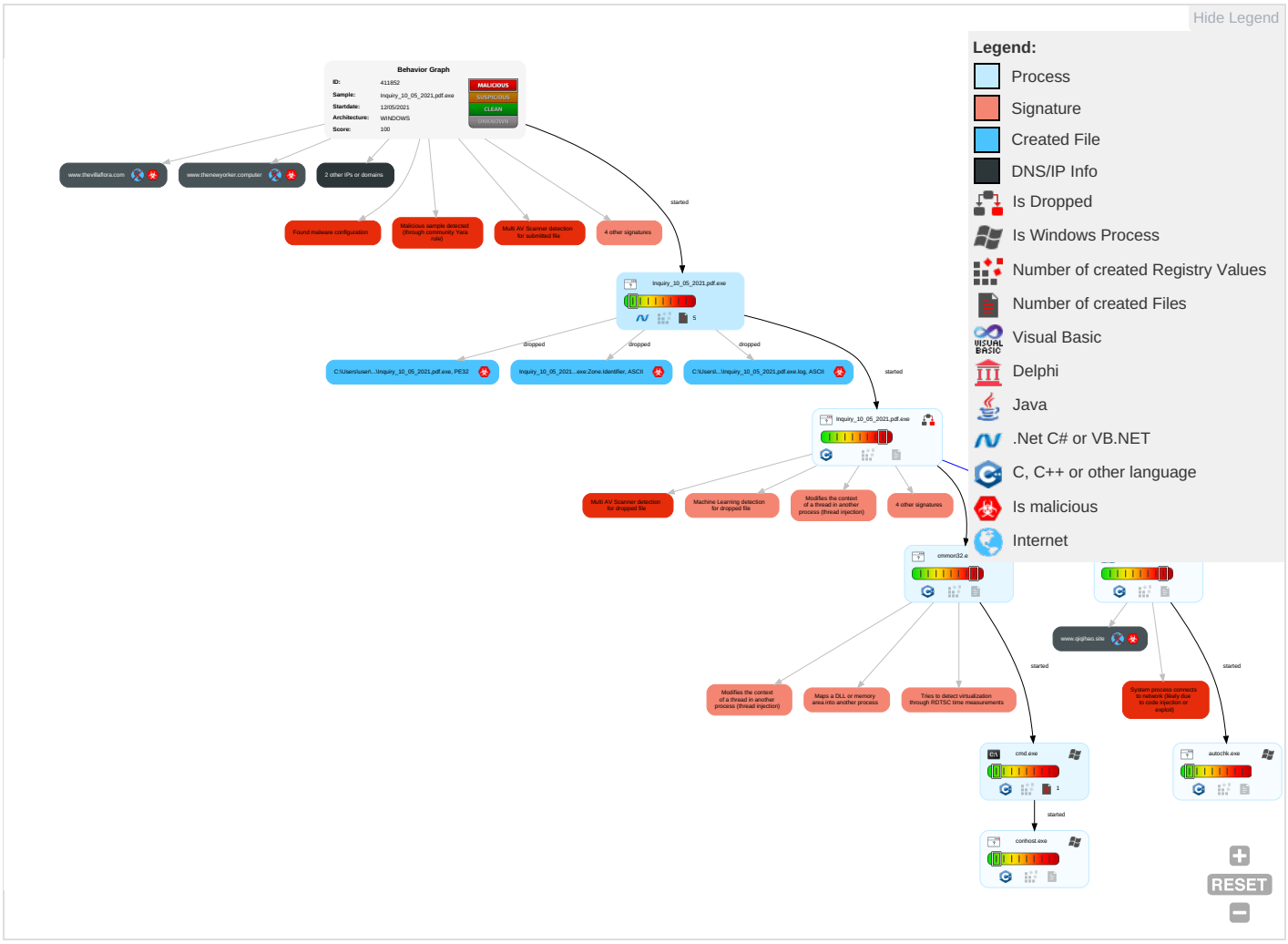
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

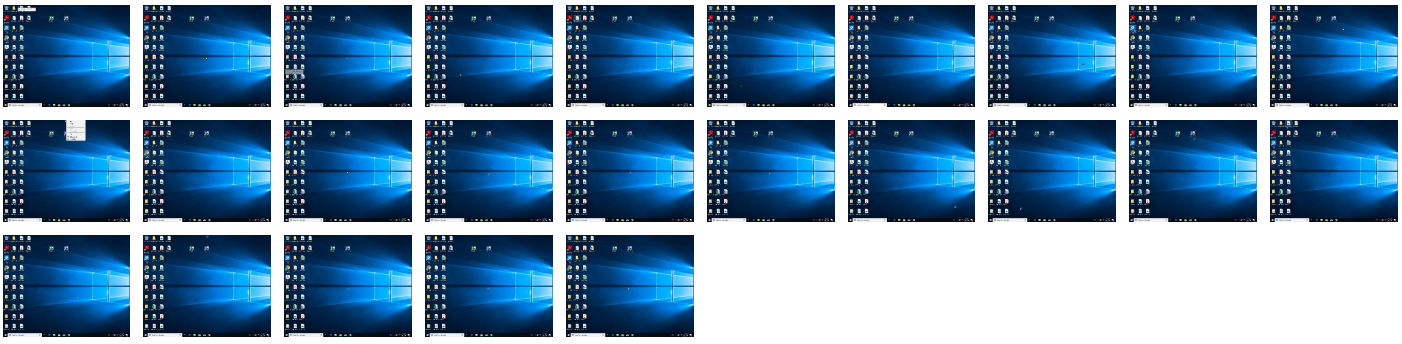
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Inquiry_10_05_2021,pdf.exe	35%	Metadefender		Browse
Inquiry_10_05_2021,pdf.exe	53%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
Inquiry_10_05_2021,pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	35%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	53%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.Inquiry_10_05_2021,pdf.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	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
www.werealestatephotography.com/hw6d/	0%	Avira URL Cloud	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
parkingpage.namecheap.com	198.54.117.215	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thevillaflora.com	192.0.78.24	true	true		unknown
www.qiqihao.site	unknown	unknown	true		unknown
www.thevillaflora.com	unknown	unknown	true		unknown
www.thenewyorker.computer	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.werealestatephotography.com/hw6d/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://james.newtonking.com/projects/json	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.328996100.00000397E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.newtonsoft.com/jsonschema	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.328996100.00000000397E000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.328996100.00000000397E000.00000004.00000001.sdmp	false		high
http://www.fonts.com	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.327976941.00000000002814000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Inquiry_10_05_2021,pdf.exe, 00000000.00000002.333247241.00000000006A22000.00000004.00000001.sdmp, explorer.exe, 0000000E.00000000.352497565.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411852
Start date:	12.05.2021
Start time:	07:48:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inquiry_10_05_2021,pdf.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:	30
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@9/3@3/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.8% (good quality ratio 9.7%) • Quality average: 72.3% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 93.184.220.29, 13.64.90.137, 23.218.208.56, 2.20.143.16, 2.20.142.209, 20.190.160.75, 20.190.160.73, 20.190.160.129, 20.190.160.134, 20.190.160.71, 20.190.160.67, 20.190.160.136, 20.190.160.69, 20.82.210.154, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/411852/sample/Inquiry_10_05_2021,pdf.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	POI09876OIUY.exe	Get hash	malicious	Browse	• 198.54.117.210
	EDS03932,pdf.exe	Get hash	malicious	Browse	• 198.54.117.216
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.117.216
	slot Charges.exe	Get hash	malicious	Browse	• 198.54.117.216
	PO09641.exe	Get hash	malicious	Browse	• 198.54.117.215
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 198.54.117.211
	Purchase Order-10764.exe	Get hash	malicious	Browse	• 198.54.117.212
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 198.54.117.218
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• 198.54.117.216
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.117.215

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 198.54.117.217
	NEW ORDER.exe	Get hash	malicious	Browse	• 198.54.117.217
	0876543123.exe	Get hash	malicious	Browse	• 198.54.117.210
	g1EhgmCqCD.exe	Get hash	malicious	Browse	• 198.54.117.216
	Payment.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	w73FtMA4ZTl9NFm.exe	Get hash	malicious	Browse	• 198.54.117.212
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.54.117.218

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inquiry_10_05_2021,pdf.exe.log	
Process:	C:\Users\user\Desktop\Inquiry_10_05_2021,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	
Process:	C:\Users\user\Desktop\Inquiry_10_05_2021,pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	551936
Entropy (8bit):	7.85215330618776
Encrypted:	false
SSDEEP:	12288:OHFMw7Y9MA59CyMAn0pGZVkfK6Jaei3kqh6PehkHFRAomlTx:OH+w09tVSKLkqh6P3lRAoqTx
MD5:	D394A8C0A37BCDAF432B2882714C6EBA
SHA1:	52D386445E50600A920F16692BBF30829D08932C
SHA-256:	3F4DC309BE69548972299CB0517C884BCB5A472FBF9693FF3D07776C9464AF1C
SHA-512:	1EBCC07FA5409255BE3803B1286C693B2271237A9B436743AB79BC3380C64428955495068864l6B6FC9F7A99B2A1133267A3B9DF9FF023BB61EF8A4674F76370
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 53%
Reputation:	low

C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....X.....w... .....@.. ..... .@.....w..J..... ..... ..H.....text....X... ...X..... ..`.rsrc.....Z.....@..@.reloc..... .....j.....@..B.....w.....H.....&..D.....;...<.....^..}.....(.....(.....*.0..e.....%-.+;+.. ....+4.-...,..+1.%,.X+-.-.++....+(+)-.+(+-.(....(....&*.+.(... .+..+..+..+..+..+.s....+..+....0..^.....+8,.+7{.....+..+-.-.++,..-...-.+#{....+...,...-.+.+.+..*.+..+..+..+..+.o....+..+..+.(....+...".(.....*...".(.....*...".(.....*...f+.+.{....+.*.+..+.o....+....0..U.. .....,.+%..+(..-.+).....s....+"..-.+#+(..-.*(....+.(....+.(....+.o....+.s....+.(....+

C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Inquiry_10_05_2021,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	
Entropy (8bit):	7.85215330618776
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Inquiry_10_05_2021,pdf.exe
File size:	551936
MD5:	d394a8c0a37bcdaf432b2882714c6eba
SHA1:	52d386445e50600a920f16692bbf30829d08932c
SHA256:	3f4dc309be69548972299cb0517c884bcb5a472fbf9693ff3d07776c9464af1c
SHA512:	1ebcc07fa5409255be3803b1286c693b2271237a9b436743ab79bc3380c64428955495068864l6b6fc9f7a99b2a1133267a3b9df9ff023bb61ef8a4674f76370
SSDEEP:	12288:OHFMw7Y9MA59CyMAn0pGZVkfK6Jaei3kqh6PehkHFRAomlTx:OH+w09tVSKLkqh6P3lRAoqTx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....X.....w... .....@.. .....@.....

File Icon

	
Icon Hash:	f6a6a68e9af2f074

Static PE Info

General

Entrypoint:	0x4777fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General	
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6098A9D5 [Mon May 10 03:34:45 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x777b0	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x10efc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x75800	0x75800	False	0.993184840426	data	7.99403499414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x10efc	0x11000	False	0.165067784926	data	5.0205162412	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	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_ICON	0x7806c	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x888d0	0x14	data		
RT_VERSION	0x88920	0x3b6	data		
RT_MANIFEST	0x88d12	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 2020 Google LLC. All rights reserved.
Assembly Version	90.0.4430.93
InternalName	Irqoouoq.exe
FileVersion	90.0.4430.93
CompanyName	Google LLC
LegalTrademarks	
Comments	Google Chrome
ProductName	Google Chrome
ProductVersion	90.0.4430.93
FileDescription	Google Chrome
OriginalFilename	Irqoouoq.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:49:21.256098986 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:21.304995060 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 07:49:21.889221907 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:21.937774897 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 07:49:23.273726940 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:23.325436115 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 07:49:24.388642073 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:24.440272093 CEST	53	55984	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:49:25.728013039 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:25.776848078 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 07:49:27.065495014 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:27.114459038 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 07:49:28.324734926 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:28.377542973 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 07:49:29.706060886 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:29.755786896 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 07:49:30.905965090 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:30.957581997 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 07:49:32.058618069 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:32.107301950 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 07:49:33.303941011 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:33.355504036 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 07:49:34.451869011 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:34.500504971 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 07:49:35.558851004 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:35.615962982 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 07:49:36.897396088 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:36.946857929 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 07:49:38.023755074 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:38.081182957 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 07:49:39.141552925 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:39.190644979 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 07:49:40.209465981 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:40.258169889 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 07:49:41.310051918 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 07:49:41.361665964 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 07:50:00.487925053 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 07:50:00.560127020 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 07:50:17.261084080 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 07:50:17.319989920 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 07:50:33.764619112 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 07:50:33.844244003 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 07:50:38.134407997 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 07:50:38.205677986 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 07:50:47.037630081 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 07:50:47.096478939 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 07:51:00.579133987 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 07:51:00.654954910 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 07:51:18.932662010 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 07:51:19.004630089 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 07:51:24.825037003 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 07:51:24.883832932 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 07:51:31.640427113 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 07:51:32.004530907 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 07:51:37.019403934 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 07:51:37.081526041 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 07:51:42.176451921 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 07:51:42.235138893 CEST	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 07:51:31.640427113 CEST	192.168.2.3	8.8.8.8	0x3fc9	Standard query (0)	www.qiqihao.site	A (IP address)	IN (0x0001)
May 12, 2021 07:51:37.019403934 CEST	192.168.2.3	8.8.8.8	0x2b80	Standard query (0)	www.thevil laflora.com	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.176451921 CEST	192.168.2.3	8.8.8.8	0x5220	Standard query (0)	www.thenew yorker.computer	A (IP address)	IN (0x0001)

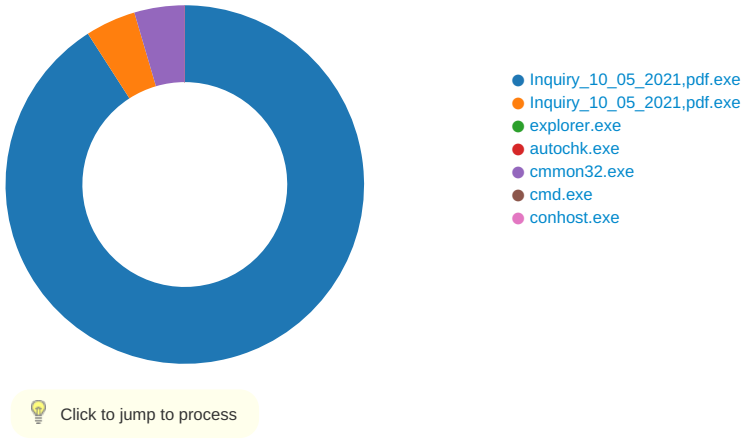
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 07:50:33.844244003 CEST	8.8.8.8	192.168.2.3	0xa9b7	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:51:32.004530907 CEST	8.8.8.8	192.168.2.3	0x3fc9	Name error (3)	www.qiqihao.site	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:51:37.081526041 CEST	8.8.8.8	192.168.2.3	0x2b80	No error (0)	www.thevillaflora.com	thevillaflora.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:51:37.081526041 CEST	8.8.8.8	192.168.2.3	0x2b80	No error (0)	thevillaflora.com		192.0.78.24	A (IP address)	IN (0x0001)
May 12, 2021 07:51:37.081526041 CEST	8.8.8.8	192.168.2.3	0x2b80	No error (0)	thevillaflora.com		192.0.78.25	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	www.thenewyorker.computer	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 12, 2021 07:51:42.235138893 CEST	8.8.8.8	192.168.2.3	0x5220	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Inquiry_10_05_2021,pdf.exe PID: 1560 Parent PID: 5680

General

Start time:	07:49:28
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Inquiry_10_05_2021,pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Inquiry_10_05_2021,pdf.exe'
Imagebase:	0x4e0000
File size:	551936 bytes
MD5 hash:	D394A8C0A37BCDAF432B2882714C6EBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.329149948.0000000003A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.329149948.0000000003A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.329149948.0000000003A30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.328783834.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.328783834.00000000037D9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.328783834.00000000037D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.328847245.000000000386E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.328847245.000000000386E000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.328847245.000000000386E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.328240255.0000000002995000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.328240255.0000000002995000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.328240255.0000000002995000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6DF6EAF6	unknown
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6DF6EAF6	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inquiry_10_05_2021,pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d5 a9 98 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 58 07 00 00 12 01 00 00 00 00 00 fa 77 07 00 00 20 00 00 00 80 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 c0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....X...........w... ....@.. ....@................	success or wait	3	6DF6EAF6	unknown
C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6DF6EAF6	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inquiry_10_05_2021,pdf.exe.log	unknown	1119	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: Inquiry_10_05_2021,pdf.exe PID: 576 Parent PID: 1560

General

Start time:	07:50:28
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe
Imagebase:	0x7a0000
File size:	551936 bytes
MD5 hash:	D394A8C0A37BCDAF432B2882714C6EBA
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.392435826.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.392435826.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.392435826.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.392729225.0000000000C90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.392729225.0000000000C90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.392729225.0000000000C90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.392783029.0000000000CE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.392783029.0000000000CE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.392783029.0000000000CE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, Metadefender, Browse • Detection: 53%, ReversingLabs
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	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 576

General

Start time:	07:50:30
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: autochk.exe PID: 2156 Parent PID: 3388

General

Start time:	07:50:46
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0x820000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmmon32.exe PID: 4772 Parent PID: 576

General

Start time:	07:50:59
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xf80000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.463820601.00000000034E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.463820601.00000000034E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.463820601.00000000034E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.463320997.0000000003270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.463320997.0000000003270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.463320997.0000000003270000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.463935334.0000000003510000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.463935334.0000000003510000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.463935334.0000000003510000.00000004.00000001.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	32882A7	NtReadFile

Analysis Process: cmd.exe PID: 5068 Parent PID: 4772

General

Start time:	07:51:00
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\Inquiry_10_05_2021,pdf.exe'
Imagebase:	0xad0000
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: 3776 Parent PID: 5068

General

Start time:	07:51:01
Start date:	12/05/2021
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