ID: 563220
Sample Name: QUOTATION PDF_SCAN_COPY.exe
Cookbook: default.jbs
Time: 12:05:21
Date: 31/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

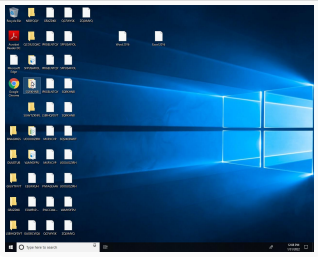
Windows Analysis Report

QUOTATION PDF_SCAN_COPY.exe

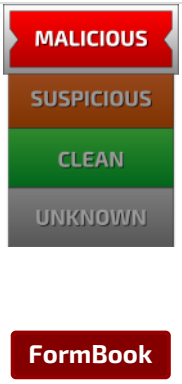
Overview

General Information

Sample Name:	QUOTATION PDF_SCAN_COPY.exe
Analysis ID:	563220
MD5:	5e9af5b2056e4d..
SHA1:	b779402e9a6ecb..
SHA256:	35147128936c2e..
Tags:	exe formbook
Infos:	



Detection



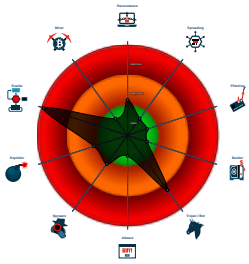
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- QUOTATION PDF_SCAN_COPY.exe (PID: 6844 cmdline: "C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe" MD5: 5E9AF5B2056E4DA639A9459E3B36193C)
  - powershell.exe (PID: 4128 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\KHDScDG.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 984 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KHDScDG" /XML "C:\Users\user\AppData\Local\Temp\tmp2DBB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - QUOTATION PDF_SCAN_COPY.exe (PID: 796 cmdline: C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe MD5: 5E9AF5B2056E4DA639A9459E3B36193C)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 1716 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 4100 cmdline: /c del "C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 5880 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.faireez.club/n2t4/"
  ],
  "decoy": [
    "livingthroughthechaos.net",
    "videobuzzmedia.com",
    "felineformulas.com",
    "theorganicbees.com",
    "bizoeflow.com",
    "gtbcked.com",
    "immortalapenft.com",
    "pacherasrl.com",
    "defunddrip.black",
    "fromefarm.com",
    "newmedicalnetwork.com",
    "nikosblue.com",
    "kaecfu.online",
    "arcane-stylish.com",
    "7ox.info",
    "osamaabuzawayed.com",
    "noemielatour.com",
    "baccaratjava.com",
    "latinfoodandwinefestival.com",
    "magiclandstudios.com",
    "shazpe.com",
    "businessmanbazar.com",
    "lifewithkatiewright.com",
    "themarketingideascatalog.com",
    "nickbrizhoops.com",
    "esportsgamertv.com",
    "delinointeriores.com",
    "connotatetechnologies.net",
    "cybomatic.cloud",
    "correctmakling.site",
    "thammydora.com",
    "ageingwellhomecare.com",
    "fleetwoodjobshop.site",
    "jakulo.com",
    "drbaren.com",
    "newpointstudio.com",
    "yxuqamnj.com",
    "spiritsyncing.net",
    "hy963app.com",
    "rnp-trading-lukoil.com",
    "bowlesuniverse.com",
    "fumigacionesecouniversal.com",
    "vulvip.com",
    "heppi.pro",
    "preetiplease.com",
    "gemini-hk.icu",
    "allyazek24.xyz",
    "blackbratapparelcompany.com",
    "immersivenm.com",
    "mystoragewarehouse.com",
    "dvjdob.icu",
    "mecanicadesuelosrancagua.one",
    "cayugacommunitysolar.com",
    "parizes.site",
    "vpsincnas.com",
    "tattoo-marketplace.online",
    "garadapatngklgamazon.com",
    "signa.info",
    "simplegourmetpa.com",
    "quintanaroopt.com",
    "studio-goettingen.com",
    "brimhi.com",
    "fabula-glass.com",
    "1049hubertrd.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000000.741535276.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000000.741535276.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000000.741535276.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.835174756.0000000000E80000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.835174756.0000000000E80000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.0.QUOTATION PDF_SCAN_COPY.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.0.QUOTATION PDF_SCAN_COPY.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.0.QUOTATION PDF_SCAN_COPY.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
11.2.QUOTATION PDF_SCAN_COPY.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
11.2.QUOTATION PDF_SCAN_COPY.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 20 entries				

Sigma Overview

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

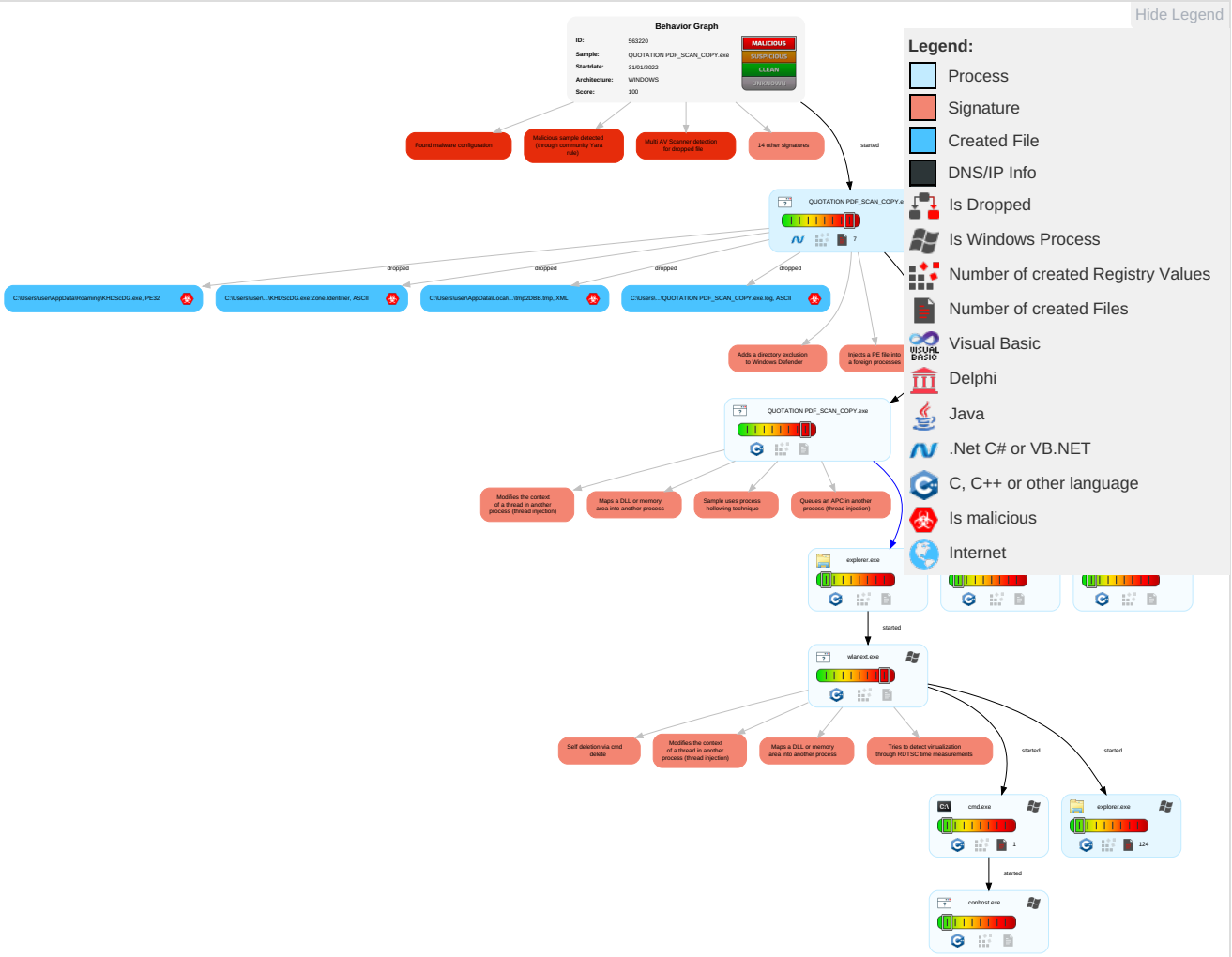
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	5 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	3 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	1 1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
QUOTATION PDF_SCAN_COPY.exe	43%	Virustotal		Browse
QUOTATION PDF_SCAN_COPY.exe	29%	Metadefender		Browse
QUOTATION PDF_SCAN_COPY.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	
QUOTATION PDF_SCAN_COPY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\KHDScDG.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\KHDScDG.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Roaming\KHDScDG.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.QUOTATION PDF_SCAN_COPY.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.0.QUOTATION PDF_SCAN_COPY.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.0.QUOTATION PDF_SCAN_COPY.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.2.QUOTATION PDF_SCAN_COPY.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.faireez.club/n2t4/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.faireez.club/n2t4/	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	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.745478312.00000000011C7000.00000004.00000020.00020000.00000000.sdmp, QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.746575972.0000000002B82000.00000004.00000800.00020000.00000000.sdmp, QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.745531520.0000000002A81000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	QUOTATION PDF_SCAN_COPY.exe, 00000001.00000002.750662294.0000000006BD2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	563220
Start date:	31.01.2022
Start time:	12:05:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION PDF_SCAN_COPY.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:	29
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@14/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.8% (good quality ratio 22.2%) • Quality average: 70.6% • Quality standard deviation: 32.7%
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

- Exclude process from analysis (whitelisted): SearchUI.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 13.107.5.88, 13.107.42.16, 23.211.5.146, 23.211.6.115, 204.79.197.200, 13.107.21.200
- Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, e12564.dspb.akamaiedge.net, config-edge-skype.l-0007.l-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, l-0007.l-msedge.net, config.edge.skype.com, storeedgefd.dsx.mp.microsoft.com, www.bing.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, l-0007.config.skype.com, store-images.s-microsoft.com, e16646.dscg.akamaiedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:06:45	API Interceptor	1x Sleep call for process: QUOTATION PDF_SCAN_COPY.exe modified
12:06:51	API Interceptor	41x Sleep call for process: powershell.exe modified

Time	Type	Description
12:08:14	API Interceptor	63x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
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\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22332
Entropy (8bit):	5.601661528735134
Encrypted:	false
SSDEEP:	384:vtCDXbqBT0BQ+KSBKncjultlK77Y9gBSJ3x6T1MaDZlbAV7/ApsSZBDI+5zg:TBABw4KcCltlfBc4CifwjUV8

MD5:	147498DB6C549710962BB6C1304E855E
SHA1:	7E5441D88801C466BC4A037E50D47D499BBA4EC9
SHA-256:	858A4B512D4D9DF5E6A33FC26E8252C55BD267AF3BD56CE0781F3DBE4A773767
SHA-512:	03C9D68D58506BFC635BF56AA3A9636E659F351D677A6304D1E4A3FD453010BC8FE66930028C9AE0CA523D6AADAAC19A5E2D51CFEAA273FD10251813E98EDF6F
Malicious:	false
Preview:	@...e.....h.a.....n...l.....@.....H.....<@.^.L."My...:X..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0flfqeem.c1z.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e0feqvz4.jvk.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2DBB.tmp

Process:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.138464141834504
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaFxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTUv
MD5:	AA21016D90C92A78024FA66167B4D7BE
SHA1:	97BF86E124F859760C7F463BEBF1A3E4FDDBE7D2
SHA-256:	4F335E7DCD45F9C9295CA77E3071616BB592079059D0B0C93B474A20418C25BE
SHA-512:	8D7D7A4E5924B556044CAE4035758912071A9D9229B4FB8914BA246EFAC1B33F0F88296FFEEC335F3053A14AB0DF9BD6650D0353487B9D01B1E25D31B1B69517
Malicious:	**true**

Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\KHDScDG.exe

Process:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	535552
Entropy (8bit):	7.39580217020087
Encrypted:	false
SSDEEP:	12288:KcqT+JVO7JUQ1h1038w3pym2sdklRwCk3:KcqcVOV3h103s0waH
MD5:	5E9AF5B2056E4DA639A9459E3B36193C
SHA1:	B779402E9A6ECBBEF6B68817814991BBCADE12DF
SHA-256:	35147128936C2E79548E5C0A2BBD70CD5A29C1B01DFA1AC2515FA5BECB7EFA6D
SHA-512:	4F293BAB428AEEAD9C4B0A411A9D0674BEBD87CF89D92F2AA0B1FFC4D287D96B859365453F21040ABC7B5DD4F452F52ED98661B8C16624D9915D4C40ECFE15EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....v.a.....0.."..... 2A... ...`....@.. ..... ..@.....@..O...`.....?..... ....H.....text...8!... ..."..... ..`.rsrc.....`.....$.....@..@.reloc.....*.....@..B.....A.....H.....,|.....0.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(.....(.....(.....(.....(.....(.....*..0.....r...p...(....r...p(.....(....r...p(.....r...p(.....(....o.....+...(.....o....r...p(.....(....-.....o.....r'..p(.....(....o.....+V..(.....>...%...%.rE..p.%..o.....o ....%.rQ..p.%...o.....%.r...p.(!

C:\Users\user\AppData\Roaming\KHDScDG.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220131\PowerShell_transcript.320946.ooSQevcZ.20220131120650.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5777
Entropy (8bit):	5.396346341966378
Encrypted:	false
SSDEEP:	96:BZqjONEUqDo1Z0TZBjONEUqDo1ZsqcSjZ4AjONEUqDo1ZNPCC8ZX:4XZGf
MD5:	05E8711C62306DB9A0825BBF92E3E028
SHA1:	791C41350092092FA293623F35C70CD0B97EEC59
SHA-256:	206403375AA38891911139183B7C118D025435E764A968E8114BA90646B34E9C
SHA-512:	4BCBA560C830AB19A6E6E78D0AFFD0AE28EFBE2006421824FD27A2EBA774DA5B3F634875C0A94BBEA4D19EF26C6DD93318A2062C2DB25554B800C80301A7D3CA
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220131120651..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\KHDScDG.exe..Process ID: 4128..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220131120651..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\KHDScDG.exe..**********..Windows PowerShell transcript start..Start time: 20220131121105..Username: computer\user..RunAs User: computer\user..Con

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.39580217020087
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:	QUOTATION PDF_SCAN_COPY.exe
File size:	535552
MD5:	5e9af5b2056e4da639a9459e3b36193c
SHA1:	b779402e9a6ecbbef6b68817814991bbcade12df
SHA256:	35147128936c2e79548e5c0a2bbd70cd5a29c1b01dfa1ac2515fa5becb7efa6d
SHA512:	4f293bab428aeead9c4b0a411a9d0674bebd87cf89d92f2aa0b1ffc4d287d96b859365453f21040abc7b5dd4f452f52ed98661b8c16624d9915d4c40ecfe15ea
SSDEEP:	12288:KcqT+JVO7JUQ1h1038w3pym2sdklRwCk3:KcqcVOV3h103s0waH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....v.a.....0..".....2A... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x484132
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:	0x61F77617 [Mon Jan 31 05:39:35 2022 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x840e0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x5e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x83fa8	0x1c	.text
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x82138	0x82200	False	0.755804965178	data	7.40361532396	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x5e4	0x600	False	0.435546875	data	4.17670383408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	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	0x86090	0x352	data		
RT_MANIFEST	0x863f4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

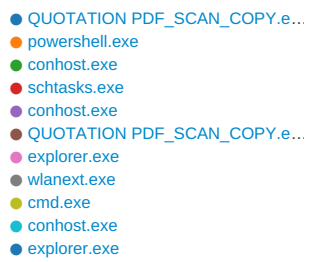
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2010 Honda Fit
Assembly Version	12.1.9.0
InternalName	Regist.exe
FileVersion	12.0.0.0
CompanyName	Honda
LegalTrademarks	
Comments	Borders Books
ProductName	LineNumberInfo
ProductVersion	12.0.0.0
FileDescription	LineNumberInfo
OriginalFilename	Regist.exe

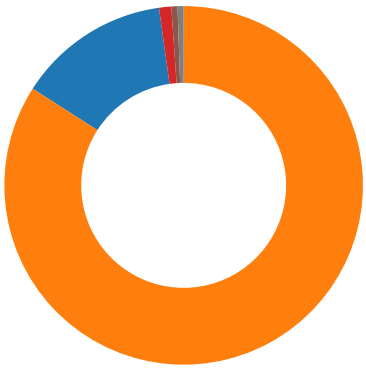
Network Behavior

No network behavior found

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: QUOTATION PDF_SCAN_COPY.exe PID: **6844**, Parent PID: **6008**

General

Target ID:	1
Start time:	12:06:19
Start date:	31/01/2022
Path:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe"
Imagebase:	0x770000
File size:	535552 bytes
MD5 hash:	5E9AF5B2056E4DA639A9459E3B36193C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.748414866.0000000003A89000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.748414866.0000000003A89000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.748414866.0000000003A89000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.746575972.0000000002B82000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.745531520.0000000002A81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **4128**, Parent PID: **6844**

General

Target ID:	7
Start time:	12:06:48
Start date:	31/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\KHDScDG.exe
Imagebase:	0x1360000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6E1ACF06	unknown
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	6E1ACF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_e0feqvz4.jvk.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CFF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_0flfqeem.c1z.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CFF1E60	CreateFileW
C:\Users\user\Documents\20220131	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFFBEFF	CreateDirectoryW
C:\Users\user\Documents\20220131\PowerShell_transcript.320946.ooSQevcZ.20220131120650.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CFF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_e0feqvz4.jvk.ps1	success or wait	1	6CFF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_0flfqeem.c1z.psm1	success or wait	1	6CFF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_e0feqvz4.jvk.ps1	0	1	31	1	success or wait	1	6CFF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_0flfqeem.c1z.psm1	0	1	31	1	success or wait	1	6CFF1B4F	WriteFile
C:\Users\user\Documents\20220131\PowerShell_transcript.320946.ooSQevcZ.20220131120650.txt	0	3	ff		success or wait	1	6CFF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220131\PowerShell_transcript.320946.ooSQevcZ.20220131120650.txt	3	674	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 33 31 31 32 30 36 35 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 32 30 39 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220131120651Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 320946 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6CFF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 14 00 00 18 00 00 00 68 0d 61 04 06 09 fd 08 fd 08 00 00 fd 00 6e 00 0a 00 49 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehanI@	success or wait	1	6E4776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 58 00 00 00 0e 00 20 00	H<@^L"My:X	success or wait	17	6E4776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E4776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E4776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E4776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 fd 01 40 00 55 00 40 00 47 00 40 00 54 01 40 00 fd 3e 40 01 fd 29 40 01 fd 3f 40 01 fd 6f 40 01 fd 6f 40 01 fd 6f 40 01 fd 3f 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 16 3b 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 1b 3b 40 01 19 3b 40 01 3b 4d 40 01 fd 44 40	@U@G@T@>@)@? @o@o@o@? @V@@@@V@H@ X@[@NT@HT@S@S@ hT@S@S@S@\@T@T @@X@? X@T@;@S@S@T@T@ xT@zT@T@=M@DM @:M@"M@ M@!M@g@@@;@;@;M @D@	success or wait	11	6E4776FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E18CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E18CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E185705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E191F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6E19203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0E03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CFF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0E03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E185705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CFF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CFF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6CFF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CFF1B4F	ReadFile

Analysis Process: conhost.exe PID: **3532**, Parent PID: **4128**

General

Target ID:	8
Start time:	12:06:49
Start date:	31/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6eb840000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **984**, Parent PID: **6844**

General

Target ID:	9
Start time:	12:06:49
Start date:	31/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KHDScDG" /XML "C:\Users\user\AppData\Local\Temp\tmp2DBB.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2DBB.tmp	unknown	2	success or wait	1	10AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2DBB.tmp	unknown	1595	success or wait	1	10AABD9	ReadFile

Analysis Process: conhost.exe PID: **3220**, Parent PID: **984**

General

Target ID:	10
Start time:	12:06:50
Start date:	31/01/2022

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

Analysis Process: QUOTATION PDF_SCAN_COPY.exe PID: **796**, Parent PID: **6844**

General

Target ID:	11
Start time:	12:06:51
Start date:	31/01/2022
Path:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe
Imagebase:	0x5a0000
File size:	535552 bytes
MD5 hash:	5E9AF5B2056E4DA639A9459E3B36193C
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: 0000000B.00000000.741535276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.741535276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.741535276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.835174756.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.835174756.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.835174756.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.741938582.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.741938582.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.741938582.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.834375246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.834375246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.834375246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.834839904.0000000000B50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.834839904.0000000000B50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.834839904.0000000000B50000.00000040.10000000.00040000.00000000.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	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3424**, Parent PID: **796**

General	
Target ID:	13
Start time:	12:06:56
Start date:	31/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.775484148.000000000DADA000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.775484148.000000000DADA000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.775484148.000000000DADA000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.794471211.000000000DADA000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.794471211.000000000DADA000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.794471211.000000000DADA000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: wlanext.exe PID: **1716**, Parent PID: **3424**

General	
Target ID:	19
Start time:	12:07:33
Start date:	31/01/2022
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x8c0000
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: 00000013.00000002.981277393.0000000003270000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.981277393.0000000003270000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.981277393.0000000003270000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.980171637.0000000000950000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.980171637.0000000000950000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.980171637.0000000000950000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.980875419.0000000002F70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.980875419.0000000002F70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.980875419.0000000002F70000.00000040.10000000.00040000.00000000.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	328A447	NtReadFile

Analysis Process: cmd.exe PID: **4100**, Parent PID: **1716**

General

Target ID:	21
Start time:	12:07:38
Start date:	31/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\QUOTATION PDF_SCAN_COPY.exe"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4680**, Parent PID: **4100**

General

Target ID:	22
Start time:	12:07:39
Start date:	31/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **5880**, Parent PID: **4116**

General

Target ID:	26
Start time:	12:08:12
Start date:	31/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6fee60000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly