ID: 626604
Sample Name: fooYgfbxno
Cookbook: default.jbs
Time: 15:27:26
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

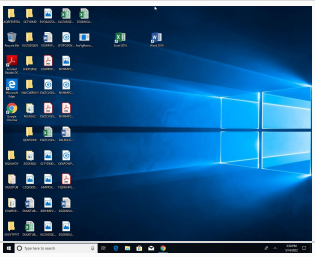
Windows Analysis Report

fooYgfbxno

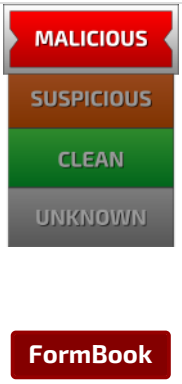
Overview

General Information

Sample Name:	fooYgfbxno (renamed file extension from none to exe)
Analysis ID:	626604
MD5:	ce42fe431b8892..
SHA1:	652914d960da1d.
SHA256:	4d8cc879424990..
Tags:	32 exe trojan
Infos:	



Detection



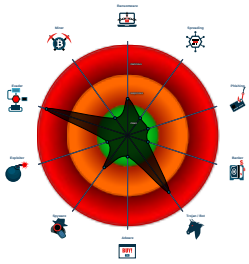
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- fooYgfbxno.exe (PID: 6212 cmdline: "C:\Users\user\Desktop\fooYgfbxno.exe" MD5: CE42FE431B88922AB59B6FD880CADCF6)
  - aspnet_compiler.exe (PID: 6324 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - svchost.exe (PID: 1988 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
      - cmd.exe (PID: 5064 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.mentalnayaarifmetika.online/ocgr/"
  ],
  "decoy": [
    "shiftmedicalstaffing.agency",
    "muktobangla.xyz",
    "attmleather.com",
    "modelahs.com",
    "clime.email",
    "yonatec.com",
    "mftie.com",
    "doxofcolor.com",
    "american-atlantic.net",
    "christineenergy.com",
    "fjqsdz.com",
    "nagpurmandarin.com",
    "hofwimmer.com",
    "gororidev.com",
    "china-eros.com",
    "xn--ekrt15fxyb2t2c.xn--czru2d",
    "dabsavy.com",
    "buggy4t.com",
    "souplant.com",
    "insurancewineappraisals.com",
    "012skz.xyz",
    "kincsemto.net",
    "zyaxious.website",
    "tellgalpy.com",
    "demetbatmaz.com",
    "wallacehills.com",
    "chambaultfleurs.com",
    "fairfieldgroupfw.com",
    "lotsimprovements.com",
    "dhslcy.com",
    "anotherdegen.com",
    "dearpennyyouradviceblogspot.com",
    "seekbeforefind.com",
    "societyalluredmcc.com",
    "climatecheckin.com",
    "candybox-eru.com",
    "tentacionescharlie.com",
    "exceedrigging.online",
    "skb-cabinet.com",
    "qhzhuhang.com",
    "ccav11.xyz",
    "sandstonehosting.com",
    "14offresimportantes.com",
    "xn--hj2bz6fwvan2be1g5tb.com",
    "embedded-electronic.com",
    "drsanaclinic.com",
    "ageofcryptos.com",
    "dreamonetnpasumo1.xyz",
    "engroconnect.net",
    "huvao.com",
    "denalicanninglids.com",
    "tootko.com",
    "edisson-bd.com",
    "myamazonloan.net",
    "dbcyebnveoyu.cloud",
    "floridacaterpillar.com",
    "travisjbogard.com",
    "dialoneconstruction.com",
    "tubesing.com",
    "gofilmwizards.com",
    "tahnforest.com",
    "salahov.info",
    "bimcellerviss.com",
    "garglimited.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.359226665.0000000001440000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.359226665.0000000001440000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.359226665.0000000001440000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.359013651.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.359013651.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.aspnet_compiler.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.aspnet_compiler.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
2.2.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.aspnet_compiler.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 16 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 61.14.208.3

Timestamp:	192.168.2.361.14.208.349768802031412 05/14/22-15:30:39.400782
SID:	2031412
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 61.14.208.3

Timestamp:	192.168.2.361.14.208.349768802031453 05/14/22-15:30:39.400782
SID:	2031453
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 61.14.208.3

Timestamp:	192.168.2.361.14.208.349768802031449 05/14/22-15:30:39.400782
SID:	2031449
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

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

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

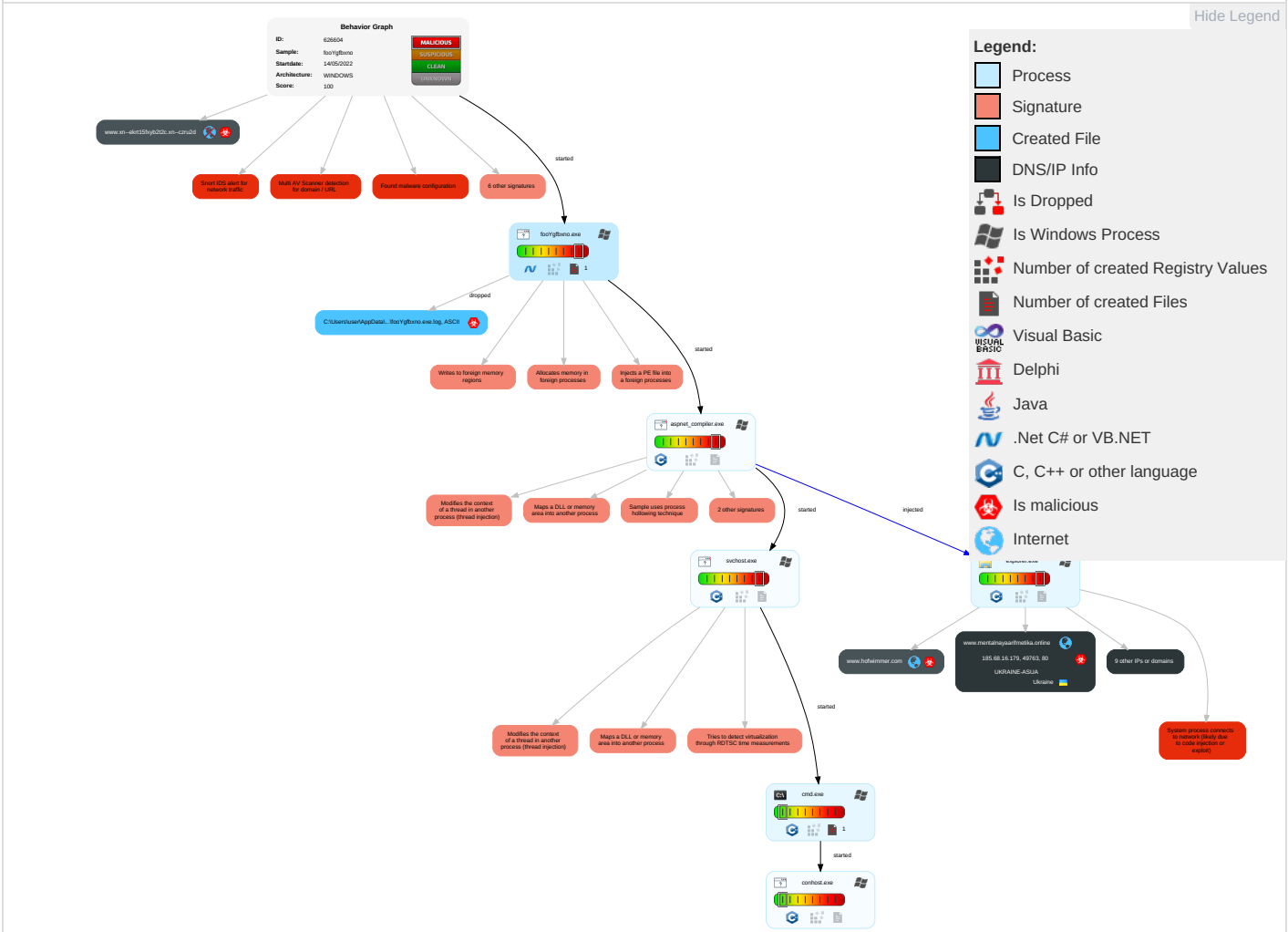
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	8 1 2 Process Injection	1 Masquerading	1 Input Capture	1 2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	8 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
fooYgfbxno.exe	32%	Virustotal		Browse
fooYgfbxno.exe	44%	ReversingLabs	Win32.Trojan.Swotter	
fooYgfbxno.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.aspnet_compiler.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.aspnet_compiler.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
lotsimprovements.com	8%	Virustotal		Browse
www.huvao.com	2%	Virustotal		Browse
www.chambaultfleurs.com	3%	Virustotal		Browse
www.xn--hj2bz6fwvan2be1g5tb.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.chambaultfleurs.com/ocgr/?lfvx9=JFNTlvkP_&P2Jl4=TZNys7210trfg8O8WBMuzy6C02l8maceBl4kNVlEZuNH+N4fd/TFP34Py3WDgrqbJJxT	100%	Avira URL Cloud	malware	
http://www.lotsimprovements.com/ocgr/?P2Jl4=o9xz2vqcTVXu/W078IUcrzT+VrP3S9wZB9suAAi9fTl7LQCsWydvJWt3Uuk2q/fLQQGI&lfvx9=JFNTlvkP_	100%	Avira URL Cloud	malware	
http://www.xn--hj2bz6fwvan2be1g5tb.com/ocgr/?lfvx9=JFNTlvkP_&P2Jl4=zPygAtD4LGfbsOxaPXlKDZlA/HZsirEX7sJv7vNHedMyDqAMsgZk6w8aA/BuIJhq09F8	100%	Avira URL Cloud	malware	
http://www.huvao.com/ocgr/?P2Jl4=1BqqsZcQDAJnvcG+ktWW1SuLtWUnTVqW01xF9ocnHpFG4dYykDk5mjpX7chd6+Nfhcmp&lfvx9=JFNTlvkP_	100%	Avira URL Cloud	malware	
www.mentalnayaarifmetika.online/ocgr/	100%	Avira URL Cloud	malware	
http://www.mentalnayaarifmetika.online/ocgr/?P2Jl4=WCPK4waC2+ZoHrOc/rbcYrxYoSsYkto1AfFtfo68nJJBD8+b6aAxZ/giJh8W0WW05dhF&lfvx9=JFNTlvkP_	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lotsimprovements.com	209.15.40.102	true	true	• 8%, Virustotal, Browse	unknown
www.huvao.com	104.21.89.61	true	true	• 2%, Virustotal, Browse	unknown
www.chambaultfleurs.com	213.186.33.5	true	true	• 3%, Virustotal, Browse	unknown
www.xn--hj2bz6fwvan2be1g5tb.com	61.14.208.3	true	true	• 4%, Virustotal, Browse	unknown
www.hofwimmer.com	206.189.50.60	true	true		unknown
www.mentalnayaarifmetika.online	185.68.16.179	true	true		unknown
www.myamazonloan.net	unknown	unknown	true		unknown
www.lotsimprovements.com	unknown	unknown	true		unknown
www.zyaxious.website	unknown	unknown	true		unknown
www.doxofcolor.com	unknown	unknown	true		unknown
www.xn--ekrt15fxyb2t2c.xn--czru2d	unknown	unknown	true		unknown

Contacted URLs

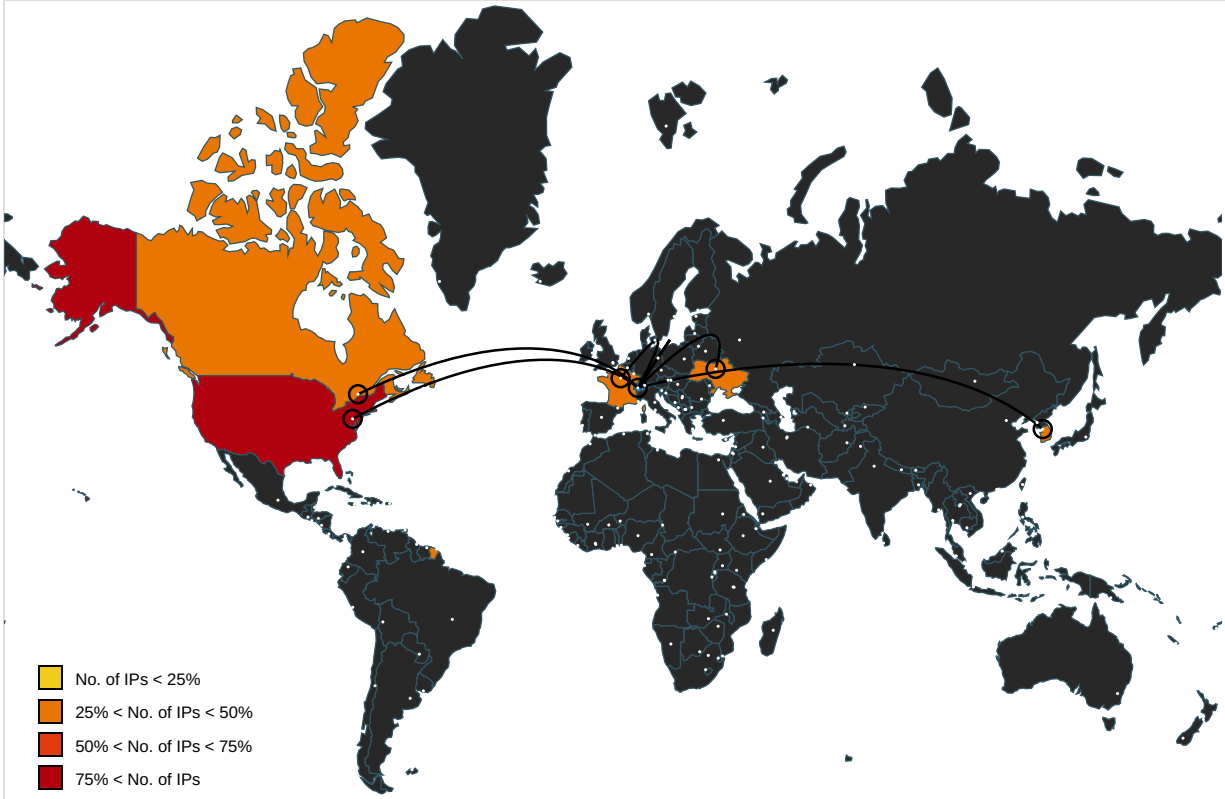
Name	Malicious	Antivirus Detection	Reputation
http://www.chambaultfleurs.com/ocgr/?lfvx9=JFNTlvkP_&P2Jl4=TZNys7210trfg8O8WBMuzy6C02l8maceBl4kNVlEZuNH+N4fd/TFP34Py3WDgrqbJJxT	true	• Avira URL Cloud: malware	unknown
http://www.lotsimprovements.com/ocgr/?P2Jl4=o9xz2vqcTVXu/W078IUcrzT+VrP3S9wZB9suAAi9fTl7LQCsWydvJWt3Uuk2q/fLQQGI&lfvx9=JFNTlvkP_	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.xn--hj2bz6fwvan2be1g5tb.com/ocgr/?lfvx9=JFNTlvkP_&P2Jl4=zPygAtD4LGfbsOxaPXlKDZlA/HZsirEX7sJv7vNHedMyDqAMsgZk6w8aA/BuIJhq09F8	true	• Avira URL Cloud: malware	unknown
http://www.huvao.com/ocgr/?P2Jl4=1BqqsZcQDAJnvcG+ktWW1SuLtWUnTVqW01xF9ocnHpFG4dYykDk5mjpX7chd6+Nfhcmp&lfvx9=JFNTlvkP_	true	• Avira URL Cloud: malware	unknown
www.mentalnayaarifmetika.online/ocgr/	true	• Avira URL Cloud: malware	low
http://www.mentalnayaarifmetika.online/ocgr/?P2Jl4=WCPK4waC2+ZoHrOc/rbcYrxYoSsYkto1AfFtfo68nJJBD8+b6aAxZ/giJh8W0WW05dhF&lfvx9=JFNTlvkP_	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://adm.tools/support/	svchost.exe, 0000000C.00000002.530690734.0000000003FB2000.00000004.10000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.89.61	www.huvao.com	United States		13335	CLOUDFLARENETUS	true
185.68.16.179	www.mentalnayaarifmetika.online	Ukraine		200000	UKRAINE-ASUA	true
213.186.33.5	www.chambaultfleurs.com	France		16276	OVHFR	true
209.15.40.102	lotsimprovements.com	Canada		13768	COGECO-PEER1CA	true
61.14.208.3	www.xn--hj2bz6fwvan2be1g5tb.com	Korea Republic of		45382	EHOSTIDC-AS-KREHOSTICTKR	true
206.189.50.60	www.hofwimmer.com	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626604

Start date and time: 14/05/202215:27:26	2022-05-14 15:27:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fooYgfbxno (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/1@10/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 53.3% (good quality ratio 48.9%) • Quality average: 73.4% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\fooYgfbxno.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.341038075456123
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21t92W+P12MUAvvrs:Q3La/KDLI4MWuPk21t92n4M6
MD5:	9FEAEEB3F595D644B8A003CA116508D1
SHA1:	E2A4B06B16147F0C77AE2839DF37E9FFEB645DBE
SHA-256:	37C92A24F9BD9FBF354209FE9DDA880B5B9C117F2CC863764EFD7F303548696D
SHA-512:	DAE054E5DB8E869347F415FA57150B352381D1EBB90CF3D67BBFF69B4B27E0F2047E24B4E2BE36EE79EE2E94E766533772E9FF61969805C3709BD94906DBF2BA
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.903722597215708
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	fooYgfbxno.exe
File size:	229376
MD5:	ce42fe431b88922ab59b6fd880cadcf6
SHA1:	652914d960da1d37d270db7f6e3b07c9d4b0e3a9
SHA256:	4d8cc87942499042195cec4fdb2fc5869d4bf98a1d827fd30fb74e82cf0fdc0f
SHA512:	62b30a77cb2ef3491abb3ec517ca966c4a9eafa0f263118ba817a4ce87f8d3cddc014bce25ff268435b7f69605e6c14b8031b482f7caf00e855964c618c609ba
SSDEEP:	3072:AZZ8kwSCcwugf3DaUrpXtKY/c3QSXCjE/jIgQW9BPnXKWIhmpCCBHhGThql:mCugfz/5t//sTXC2b3rPXahqC
TLSH:	FA2402A067E9DF27C38D3BB2981A2B913338D502B717BF1B640904BDCC537D854E9656
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....~b.....v...|..... .....@.. .....`

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4395ca
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x627E1FBA [Fri May 13 09:07:06 2022 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
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

Instruction
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	0x39570	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c000	0x5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x35018	0x1c	.text
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	0x375d0	0x37600	False	0.946846783296	data	7.92488075838	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x3a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x3c000	0x5c8	0x600	False	0.422526041667	data	4.17915724205	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3c0a0	0x33c	data		
RT_MANIFEST	0x3c3dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

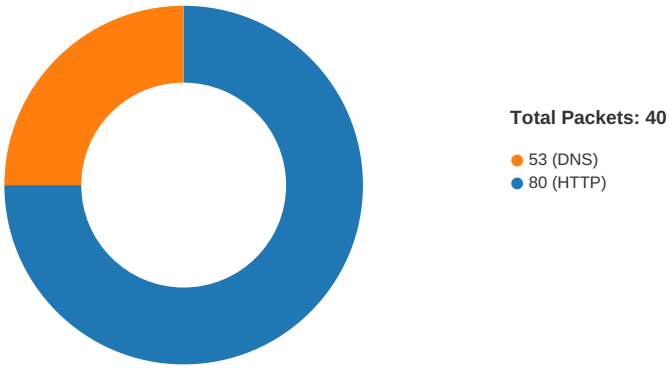
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2022
Assembly Version	1.0.0.0
InternalName	BMCXBMXCKSKS.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	BMCXBMXCKSKS
ProductVersion	1.0.0.0
FileDescription	BMCXBMXCKSKS
OriginalFilename	BMCXBMXCKSKS.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.361.14.208.349768802031412 05/14/22-15:30:39.400782	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.3	61.14.208.3
192.168.2.361.14.208.349768802031453 05/14/22-15:30:39.400782	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.3	61.14.208.3
192.168.2.361.14.208.349768802031449 05/14/22-15:30:39.400782	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.3	61.14.208.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:30:02.216365099 CEST	49760	80	192.168.2.3	104.21.89.61
May 14, 2022 15:30:02.249017000 CEST	80	49760	104.21.89.61	192.168.2.3
May 14, 2022 15:30:02.249130011 CEST	49760	80	192.168.2.3	104.21.89.61
May 14, 2022 15:30:02.249274015 CEST	49760	80	192.168.2.3	104.21.89.61
May 14, 2022 15:30:02.280647039 CEST	80	49760	104.21.89.61	192.168.2.3
May 14, 2022 15:30:02.290631056 CEST	80	49760	104.21.89.61	192.168.2.3
May 14, 2022 15:30:02.294136047 CEST	49760	80	192.168.2.3	104.21.89.61
May 14, 2022 15:30:02.325537920 CEST	80	49760	104.21.89.61	192.168.2.3
May 14, 2022 15:30:02.530217886 CEST	80	49760	104.21.89.61	192.168.2.3
May 14, 2022 15:30:02.530329943 CEST	49760	80	192.168.2.3	104.21.89.61
May 14, 2022 15:30:12.656078100 CEST	49763	80	192.168.2.3	185.68.16.179
May 14, 2022 15:30:12.699554920 CEST	80	49763	185.68.16.179	192.168.2.3
May 14, 2022 15:30:12.699672937 CEST	49763	80	192.168.2.3	185.68.16.179
May 14, 2022 15:30:12.699805021 CEST	49763	80	192.168.2.3	185.68.16.179
May 14, 2022 15:30:12.743258953 CEST	80	49763	185.68.16.179	192.168.2.3
May 14, 2022 15:30:12.743716955 CEST	80	49763	185.68.16.179	192.168.2.3
May 14, 2022 15:30:12.743794918 CEST	80	49763	185.68.16.179	192.168.2.3
May 14, 2022 15:30:12.743937016 CEST	49763	80	192.168.2.3	185.68.16.179
May 14, 2022 15:30:12.747823954 CEST	49763	80	192.168.2.3	185.68.16.179
May 14, 2022 15:30:12.791331053 CEST	80	49763	185.68.16.179	192.168.2.3
May 14, 2022 15:30:17.808177948 CEST	49764	80	192.168.2.3	213.186.33.5
May 14, 2022 15:30:17.837434053 CEST	80	49764	213.186.33.5	192.168.2.3
May 14, 2022 15:30:17.837635040 CEST	49764	80	192.168.2.3	213.186.33.5
May 14, 2022 15:30:17.837791920 CEST	49764	80	192.168.2.3	213.186.33.5
May 14, 2022 15:30:17.867481947 CEST	80	49764	213.186.33.5	192.168.2.3
May 14, 2022 15:30:17.867533922 CEST	80	49764	213.186.33.5	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:30:17.867758036 CEST	49764	80	192.168.2.3	213.186.33.5
May 14, 2022 15:30:17.867816925 CEST	49764	80	192.168.2.3	213.186.33.5
May 14, 2022 15:30:17.896970034 CEST	80	49764	213.186.33.5	192.168.2.3
May 14, 2022 15:30:28.312823057 CEST	49765	80	192.168.2.3	206.189.50.60
May 14, 2022 15:30:28.353809118 CEST	80	49765	206.189.50.60	192.168.2.3
May 14, 2022 15:30:28.353918076 CEST	49765	80	192.168.2.3	206.189.50.60
May 14, 2022 15:30:28.354022026 CEST	49765	80	192.168.2.3	206.189.50.60
May 14, 2022 15:30:28.394854069 CEST	80	49765	206.189.50.60	192.168.2.3
May 14, 2022 15:30:28.396599054 CEST	80	49765	206.189.50.60	192.168.2.3
May 14, 2022 15:30:28.396655083 CEST	80	49765	206.189.50.60	192.168.2.3
May 14, 2022 15:30:28.396800041 CEST	49765	80	192.168.2.3	206.189.50.60
May 14, 2022 15:30:28.396851063 CEST	49765	80	192.168.2.3	206.189.50.60
May 14, 2022 15:30:28.437733889 CEST	80	49765	206.189.50.60	192.168.2.3
May 14, 2022 15:30:33.578761101 CEST	49767	80	192.168.2.3	209.15.40.102
May 14, 2022 15:30:33.678956032 CEST	80	49767	209.15.40.102	192.168.2.3
May 14, 2022 15:30:33.679131985 CEST	49767	80	192.168.2.3	209.15.40.102
May 14, 2022 15:30:33.679238081 CEST	49767	80	192.168.2.3	209.15.40.102
May 14, 2022 15:30:33.779376984 CEST	80	49767	209.15.40.102	192.168.2.3
May 14, 2022 15:30:33.779448032 CEST	80	49767	209.15.40.102	192.168.2.3
May 14, 2022 15:30:33.779484987 CEST	80	49767	209.15.40.102	192.168.2.3
May 14, 2022 15:30:33.779680967 CEST	49767	80	192.168.2.3	209.15.40.102
May 14, 2022 15:30:33.779741049 CEST	49767	80	192.168.2.3	209.15.40.102
May 14, 2022 15:30:33.879672050 CEST	80	49767	209.15.40.102	192.168.2.3
May 14, 2022 15:30:39.118415117 CEST	49768	80	192.168.2.3	61.14.208.3
May 14, 2022 15:30:39.400279045 CEST	80	49768	61.14.208.3	192.168.2.3
May 14, 2022 15:30:39.400459051 CEST	49768	80	192.168.2.3	61.14.208.3
May 14, 2022 15:30:39.400782108 CEST	49768	80	192.168.2.3	61.14.208.3
May 14, 2022 15:30:39.682413101 CEST	80	49768	61.14.208.3	192.168.2.3
May 14, 2022 15:30:39.686490059 CEST	80	49768	61.14.208.3	192.168.2.3
May 14, 2022 15:30:39.686532974 CEST	80	49768	61.14.208.3	192.168.2.3
May 14, 2022 15:30:39.686790943 CEST	49768	80	192.168.2.3	61.14.208.3
May 14, 2022 15:30:39.686932087 CEST	49768	80	192.168.2.3	61.14.208.3
May 14, 2022 15:30:39.968940973 CEST	80	49768	61.14.208.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:29:57.018431902 CEST	65358	53	192.168.2.3	8.8.8.8
May 14, 2022 15:29:57.039163113 CEST	53	65358	8.8.8.8	192.168.2.3
May 14, 2022 15:30:02.187118053 CEST	53802	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:02.212249041 CEST	53	53802	8.8.8.8	192.168.2.3
May 14, 2022 15:30:07.308743954 CEST	65266	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:07.481030941 CEST	53	65266	8.8.8.8	192.168.2.3
May 14, 2022 15:30:12.526714087 CEST	63548	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:12.654772997 CEST	53	63548	8.8.8.8	192.168.2.3
May 14, 2022 15:30:17.764430046 CEST	49327	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:17.807101965 CEST	53	49327	8.8.8.8	192.168.2.3
May 14, 2022 15:30:22.914521933 CEST	51391	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:23.257592916 CEST	53	51391	8.8.8.8	192.168.2.3
May 14, 2022 15:30:28.291429043 CEST	58981	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:28.311923981 CEST	53	58981	8.8.8.8	192.168.2.3
May 14, 2022 15:30:33.409121037 CEST	61380	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:33.577389002 CEST	53	61380	8.8.8.8	192.168.2.3
May 14, 2022 15:30:38.794498920 CEST	63146	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:39.116885900 CEST	53	63146	8.8.8.8	192.168.2.3
May 14, 2022 15:30:44.699068069 CEST	58625	53	192.168.2.3	8.8.8.8
May 14, 2022 15:30:45.482522011 CEST	53	58625	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 15:29:57.018431902 CEST	192.168.2.3	8.8.8.8	0x15db	Standard query (0)	www.doxofcolor.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:02.187118053 CEST	192.168.2.3	8.8.8.8	0xfb0e	Standard query (0)	www.huvao.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:07.308743954 CEST	192.168.2.3	8.8.8.8	0x11dd	Standard query (0)	www.myamazonloan.net	A (IP address)	IN (0x0001)
May 14, 2022 15:30:12.526714087 CEST	192.168.2.3	8.8.8.8	0xe8d6	Standard query (0)	www.mentalnayaarifmetika.online	A (IP address)	IN (0x0001)
May 14, 2022 15:30:17.764430046 CEST	192.168.2.3	8.8.8.8	0x704d	Standard query (0)	www.chambaultfleurs.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:22.914521933 CEST	192.168.2.3	8.8.8.8	0x31c3	Standard query (0)	www.zyaxious.website	A (IP address)	IN (0x0001)
May 14, 2022 15:30:28.291429043 CEST	192.168.2.3	8.8.8.8	0x6d5e	Standard query (0)	www.hofwimmer.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:33.409121037 CEST	192.168.2.3	8.8.8.8	0xb05b	Standard query (0)	www.lotsimprovements.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:38.794498920 CEST	192.168.2.3	8.8.8.8	0x5598	Standard query (0)	www.xn--hj2bz6fwvan2be1g5tb.com	A (IP address)	IN (0x0001)
May 14, 2022 15:30:44.699068069 CEST	192.168.2.3	8.8.8.8	0xd859	Standard query (0)	www.xn--ekrt15fxyb2t2c.xn--czru2d	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 15:29:57.039163113 CEST	8.8.8.8	192.168.2.3	0x15db	Name error (3)	www.doxofcolor.com	none	none	A (IP address)	IN (0x0001)
May 14, 2022 15:30:02.212249041 CEST	8.8.8.8	192.168.2.3	0xfb0e	No error (0)	www.huvao.com		104.21.89.61	A (IP address)	IN (0x0001)
May 14, 2022 15:30:02.212249041 CEST	8.8.8.8	192.168.2.3	0xfb0e	No error (0)	www.huvao.com		172.67.138.124	A (IP address)	IN (0x0001)
May 14, 2022 15:30:07.481030941 CEST	8.8.8.8	192.168.2.3	0x11dd	Server failure (2)	www.myamazonloan.net	none	none	A (IP address)	IN (0x0001)
May 14, 2022 15:30:12.654772997 CEST	8.8.8.8	192.168.2.3	0xe8d6	No error (0)	www.mentalnayaarifmetika.online		185.68.16.179	A (IP address)	IN (0x0001)
May 14, 2022 15:30:17.807101965 CEST	8.8.8.8	192.168.2.3	0x704d	No error (0)	www.chambaultfleurs.com		213.186.33.5	A (IP address)	IN (0x0001)
May 14, 2022 15:30:28.311923981 CEST	8.8.8.8	192.168.2.3	0x6d5e	No error (0)	www.hofwimmer.com		206.189.50.60	A (IP address)	IN (0x0001)
May 14, 2022 15:30:28.311923981 CEST	8.8.8.8	192.168.2.3	0x6d5e	No error (0)	www.hofwimmer.com		167.99.246.105	A (IP address)	IN (0x0001)
May 14, 2022 15:30:33.577389002 CEST	8.8.8.8	192.168.2.3	0xb05b	No error (0)	www.lotsimprovements.com	lotsimprovements.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:30:33.577389002 CEST	8.8.8.8	192.168.2.3	0xb05b	No error (0)	lotsimprovements.com		209.15.40.102	A (IP address)	IN (0x0001)
May 14, 2022 15:30:39.116885900 CEST	8.8.8.8	192.168.2.3	0x5598	No error (0)	www.xn--hj2bz6fwvan2be1g5tb.com		61.14.208.3	A (IP address)	IN (0x0001)
May 14, 2022 15:30:45.482522011 CEST	8.8.8.8	192.168.2.3	0xd859	Name error (3)	www.xn--ekrt15fxyb2t2c.xn--czru2d	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.huvao.com
- www.mentalnayaarifmetika.online
- www.chambaultfleurs.com
- www.hofwimmer.com
- www.lotsimprovements.com
- www.xn--hj2bz6fwvan2be1g5tb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49760	104.21.89.61	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:02.249274015 CEST	8762	OUT	GET /ocgr/?P2Jl4=1BqqsZcQDAJnvcG+ktWW1SuLtWUnTVqW01xF9ocnHpFG4dYykDk5mjpX7chd6+Nfhcmp&lfvx9=JFNTlvkP_ HTTP/1.1 Host: www.huvao.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:02.290631056 CEST	8762	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 14 May 2022 13:30:02 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Sat, 14 May 2022 14:30:02 GMT Location: https://www.huvao.com/ocgr/?P2Jl4=1BqqsZcQDAJnvcG+ktWW1SuLtWUnTVqW01xF9ocnHpFG4dYykDk5mjpX7chd6+Nfhcmp&lfvx9=JFNTlvkP_ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Q42DbjIfw3LlkGb9yMhX4sSv0WUglUoM4DrB%2BxG45w4YrZy%2FRAUfNe5OQ5EL2dP8Tekk8Vs22dE1kRSsb2yRyov88YvGerINKGpdDZiwAWbs6TefP2d%2BRyQutarG6uGH"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 70b3fc742e2c7198-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49763	185.68.16.179	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:12.699805021 CEST	9366	OUT	GET /ocgr/?P2Jl4=WCPK4waC2+ZoHrOc/rbcYrxYoSsYkto1AfFtfo68nJJBD8+b6aAxZ/giJh8W0WW05dhF&lfvx9=JFNTlvkP_ HTTP/1.1 Host: www.mentalnayaarifmetika.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:12.743716955 CEST	9368	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Sat, 14 May 2022 13:30:12 GMT Content-Type: text/html Content-Length: 1893 Connection: close ETag: "627ea693-765" x-ray: p988:0.001/wn1005:0.000/ Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 20 2d 20 d0 a1 d1 82 d1 80 d0 b0 d0 bd d0 b8 d1 86 d0 b0 20 d0 b7 d0 b0 d0 b1 d0 bb d0 be d0 ba d0 b8 d1 80 d0 be d0 b2 d0 b0 d0 bd d0 b0 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 34 30 30 2c 37 30 30 26 73 75 62 73 65 74 3d 6c 61 74 69 6e 2c 63 79 72 69 6c 6c 69 63 27 20 72 65 6c 3d 27 73 74 79 6c 65 73 68 65 65 74 27 20 74 79 70 65 3d 27 74 65 78 74 2f 63 73 73 27 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 31 66 34 66 35 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 37 34 37 34 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 4f 70 65 6e 20 53 61 6e 73 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 65 72 72 6f 72 5f 63 6f 64 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 39 32 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 32 35 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 65 72 72 6f 72 5f 62 72 69 65 66 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 35 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 20 77 69 64 74 68 3a 20 31 30 30 25 3b 22 3e 0a 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 2d 63 65 6c 6c 3b 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 6d 69 64 64 6c 65 3b 20 70 61 64 64 69 6e 67 3a 20 30 20 34 30 70 78 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 20 77 69 64 74 68 3a 20 35 32 30 70 78 3b 22 3e 0a 20 20 20 20 20 20 20 20 Data Ascii: <!doctype html><html><head> <title>403 Forbidden - </title> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width"> <link href='https://fonts.googleapis.com/css?family=Open+Sans:400,700&subset=latin,cyrillic' rel='stylesheet' type='text/css'> <style> body { background-color: #f1f4f5; color: #37474f; line-height: 1.4; font-family: 'Open Sans', sans-serif; margin: 0; padding: 0; } .error_code { display: block; font-size: 92px; font-weight: 700; margin-top: -25px; } .error_brief { display: block; font-size: 18px; font-weight: 700; margin-bottom: 15px; } </style></head><body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49764	213.186.33.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:17.837791920 CEST	9369	OUT	GET /ocgr/?lfvx9=JFNTlvkP_&P2Jl4=TZNys7210trfg8O8WBMuzy6C02l8maceBl4kNVlEZuNH+N4fd/TFP34Py3WDgrqbJJxT HTTP/1.1 Host: www.chambaultfleurs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:17.867481947 CEST	9370	IN	HTTP/1.1 302 Moved Temporarily server: nginx date: Sat, 14 May 2022 13:30:16 GMT content-type: text/html content-length: 138 location: http://www.chambaultfleurs.com x-iplb-request-id: 66818F37:C264_D5BA2105:0050_627FAEE9_3C99E51A:3005 x-iplb-instance: 16976 set-cookie: SERVERID77446=200174|Yn+u7|Yn+u7; path=/; HttpOnly connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49765	206.189.50.60	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:28.354022026 CEST	9371	OUT	GET /ocgr/?lfvx9=JFNTlvkP_&P2Jl4=yHjxPQMm3JcJX2wgLRnbME7+3RpzNlr7I3qSF8qv7PZk+uQof5Nzr3YLke9JRpMCS0ME HTTP/1.1 Host: www.hofwimmer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:28.396599054 CEST	9372	IN	HTTP/1.1 301 Moved Permanently Age: 182 Cache-Control: public, max-age=0, must-revalidate Content-Length: 46 Content-Type: text/plain Date: Sat, 14 May 2022 13:27:26 GMT Location: https://www.hofwimmer.com/ocgr/?lfvx9=JFNTlvkP_&P2Jl4=yHjxPQMm3JcJX2wgLRnbME7+3RpzNlr7I3qSF8qv7PZk+uQof5Nzr3YLke9JRpMCS0ME Server: Netlify X-Nf-Request-Id: 01G31C6TMMWQDCFJXR36HGP811 Connection: close Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 6f 66 77 69 6d 6d 65 72 2e 63 6f 6d 2f 6f 63 67 72 2f Data Ascii: Redirecting to https://www.hofwimmer.com/ocgr/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49767	209.15.40.102	80	C:\Windows\explorer.exe

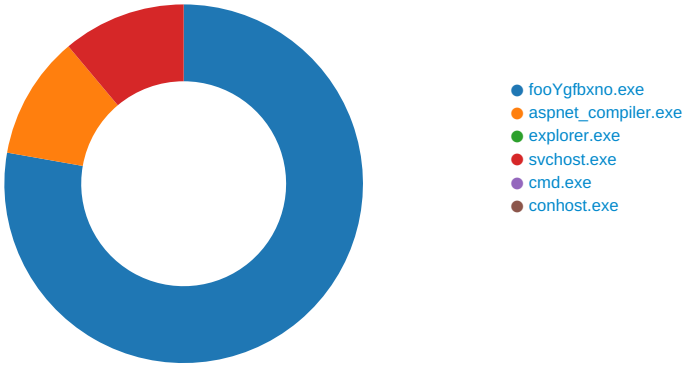
Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:33.679238081 CEST	9381	OUT	GET /ocgr/?P2Jl4=o9xz2vqcTVXu/W078IUcrzT+VrP3S9wZB9suAAi9fTl7LQCsWydvJWt3Uuk2q/fLQQGI&lfvx9=JFNTlvkP_ HTTP/1.1 Host: www.lotsimprovements.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:33.779448032 CEST	9381	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Sat, 14 May 2022 13:30:33 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.lotsimprovements.com/ocgr/?P2Jl4=o9xz2vqcTVXu/W078IUcrzT+VrP3S9wZB9suAAi9fTl7LQCsWydvJWt3Uuk2q/fLQQGI&lfvx9=JFNTlvkP_ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49768	61.14.208.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:30:39.400782108 CEST	9383	OUT	GET /ocgr/?lfvx9=JFNTlvkP_&P2Jl4=zPygAtD4LGfbsOxaPXlKDZIA/HZsirEX7sJv7vNHedMyDqAMsgZk6w8aA/BuIJhq09F8 HTTP/1.1 Host: www.xn--hj2bz6fwvan2be1g5tb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 15:30:39.686490059 CEST	9383	IN	HTTP/1.1 200 OK Date: Sat, 14 May 2022 13:25:25 GMT Server: Apache/2.4.7 (Ubuntu) Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: fooYgfbxno.exe PID: 6212, Parent PID: 4968

General

Target ID:	1
Start time:	15:28:36
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\fooYgfbxno.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\fooYgfbxno.exe"
Imagebase:	0x7f0000
File size:	229376 bytes
MD5 hash:	CE42FE431B88922AB59B6FD880CADCF6
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: 00000001.00000002.273482433.00000000041A7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.273482433.00000000041A7000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.273482433.00000000041A7000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: aspnet_compiler.exe PID: 6324, Parent PID: 6212

General

Target ID:	2
Start time:	15:28:37
Start date:	14/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xbd0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.359226665.0000000001440000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.359226665.0000000001440000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.359226665.0000000001440000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.359013651.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.359013651.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.359013651.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.359257959.0000000001470000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.359257959.0000000001470000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.359257959.0000000001470000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.267043761.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.267043761.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.267043761.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.267329216.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.267329216.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.267329216.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186C7	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6324**

General

Target ID:	3
Start time:	15:28:40
Start date:	14/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.311031707.0000000007126000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.311031707.0000000007126000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.311031707.0000000007126000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.295364991.0000000007126000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.295364991.0000000007126000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.295364991.0000000007126000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1988**, Parent PID: **6324**

General

Target ID:	12
Start time:	15:29:20
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xcb0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
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: 0000000C.00000002.529429210.00000000034D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.529429210.00000000034D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.529429210.00000000034D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.528926429.0000000000C60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.528926429.0000000000C60000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.528926429.0000000000C60000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.529505063.0000000003500000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.529505063.0000000003500000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.529505063.0000000003500000.00000004.00000800.00020000.00000000.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	C786C7	NtReadFile

Analysis Process: cmd.exe PID: **5064**, Parent PID: **1988**

General

Target ID:	13
Start time:	15:29:22
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"
Imagebase:	0xc20000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4804**, Parent PID: **5064**

General

Target ID:	14
Start time:	15:29:23
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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

No disassembly