ID: 780222
Sample Name: Order 20233.exe
Cookbook: default.jbs
Time: 16:21:13
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Order 20233.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 4
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Exploits 6
Networking 6
E-Banking Fraud 6
System Summary 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Order 20233.exe.log 12
C:\Users\user\AppData\Local\Temp\4184-48M 13
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 14
Sections 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 16
Statistics 16

Behavior 16
System Behavior 16
Analysis Process: Order 20233.exePID: 5872, Parent PID: 3452 16
General 16
File Activities 17
Analysis Process: aspnet_compiler.exePID: 6120, Parent PID: 5872 17
General 17
Analysis Process: AddInProcess.exePID: 2140, Parent PID: 5872 17
General 17
Analysis Process: Microsoft.Workflow.Compiler.exePID: 1360, Parent PID: 5872 17
General 17
Analysis Process: dfsvc.exePID: 2288, Parent PID: 5872 18
General 18
Analysis Process: aspnet_wp.exePID: 2104, Parent PID: 5872 18
General 18
Analysis Process: aspnet_regsql.exePID: 5300, Parent PID: 5872 18
General 18
Analysis Process: aspnet_regiis.exePID: 1760, Parent PID: 5872 18
General 18
Analysis Process: mscorsvw.exePID: 3956, Parent PID: 5872 19
General 19
Analysis Process: ngen.exePID: 5612, Parent PID: 5872 19
General 19
Analysis Process: AddInProcess32.exePID: 4392, Parent PID: 5872 19
General 19
File Activities 20
File Read 20
Analysis Process: explorer.exePID: 3452, Parent PID: 4392 20
General 20
File Activities 20
Analysis Process: mstsc.exePID: 5380, Parent PID: 3452 20
General 20
File Activities 21
File Deleted 21
File Read 21
Registry Activities 21
Disassembly 21

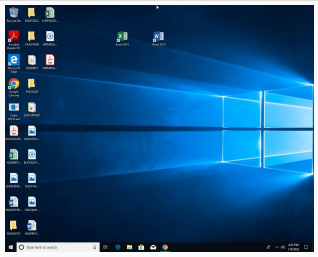
Windows Analysis Report

Order 20233.exe

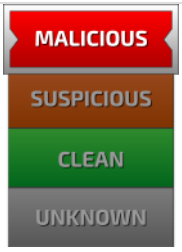
Overview

General Information

Sample Name:	Order 20233.exe
Analysis ID:	780222
MD5:	cfc3542e983b4a...
SHA1:	c792d80b3667ba..
SHA256:	614490e3bf7cf06..
Tags:	exe formbook
Infos:	



Detection



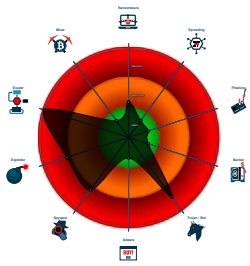
FormBook

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

Signatures

- Yara detected UAC Bypass using C...
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through...
- Yara detected AntiVM3
- System process connects to networ...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Snort IDS alert for network traffic
- Sample uses process hollowing tech...
- Tries to steal Mail credentials (via fi...
- Maps a DLL or memory area into an...

Classification



Process Tree

- **System is w10x64**
- Order 20233.exe (PID: 5872 cmdline: C:\Users\user\Desktop\Order 20233.exe MD5: CFC3542E983B4A7436DABB73132CBBDB)
  - aspnet_compiler.exe (PID: 6120 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_compiler.exe MD5: 7809A19AA8DA1A41F36B60B0664C4E20)
  - AddInProcess.exe (PID: 2140 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess.exe MD5: 11D8A500C4C0FBAF20EBDB8CDF6EA452)
  - Microsoft.Workflow.Compiler.exe (PID: 1360 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe MD5: D91462AE31562E241AF5595BA5E1A3C4)
  - dfsvc.exe (PID: 2288 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe MD5: 48FD4DD682051712E3E7757C525DED71)
  - aspnet_wp.exe (PID: 2104 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_wp.exe MD5: 3F68BCF536EEAE067038C67022CDF6D8)
  - aspnet_regsql.exe (PID: 5300 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regsql.exe MD5: F31014EE4DE7FE48E9B7C9BE94CFB45F)
  - aspnet_regiis.exe (PID: 1760 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe MD5: 061D8C0371566D560C5B15C77A34046F)
  - mscorsvw.exe (PID: 3956 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe MD5: B00E9325AC7356A3F4864EAAAD48E13F)
  - ngen.exe (PID: 5612 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe MD5: FBA5E8D94C9EADC279BC06B9CF041A9A)
  - AddInProcess32.exe (PID: 4392 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 5380 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ahmedo.ch/dcn0/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6611:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f080:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa8af:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17de7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17be5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17691:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17ce7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17e5f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa47a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x168dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1ddf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a0e9:$sqlite3step: 68 34 1C 7B E1 • 0x1ac61:$sqlite3step: 68 34 1C 7B E1 • 0x1a12b:$sqlite3text: 68 38 2A 90 C5 • 0x1aca6:$sqlite3text: 68 38 2A 90 C5 • 0x1a142:$sqlite3blob: 68 53 D8 7F 8C • 0x1acbc:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Order 20233.exe.21700429a18.0.raw.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.2.Order 20233.exe.21700429a18.0.raw.unpack	INDICATOR_SUSPICIOUS_DisableWinDefender	Detects executables containing artifcats associated with disabling Widnows Defender	ditekSHen	• 0x9c39:$e1: Microsoft\Windows Defender\Exclusions\Paths • 0x9c68:$e2: Add-MpPreference -ExclusionPath
0.2.Order 20233.exe.21700429a18.0.raw.unpack	INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM	Detects executables embedding command execution via IExecuteCommand COM object	ditekSHen	• 0x9c09:$r1: Classes\Folder\shell\open\command • 0x9058:$k1: DelegateExecute

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 213.239.221.71

Timestamp:	192.168.2.3213.239.221.7149698802031412 01/08/23-16:24:08.929621
SID:	2031412
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 213.239.221.71

Timestamp:	192.168.2.3213.239.221.7149698802031449 01/08/23-16:24:08.929621
SID:	2031449
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 213.239.221.71	−
Timestamp:	192.168.2.3213.239.221.7149698802031453 01/08/23-16:24:08.929621
SID:	2031453
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL

Exploits

- Yara detected UAC Bypass using CMSTP

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- 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
- .NET source code contains very large strings

Malware Analysis System Evasion

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

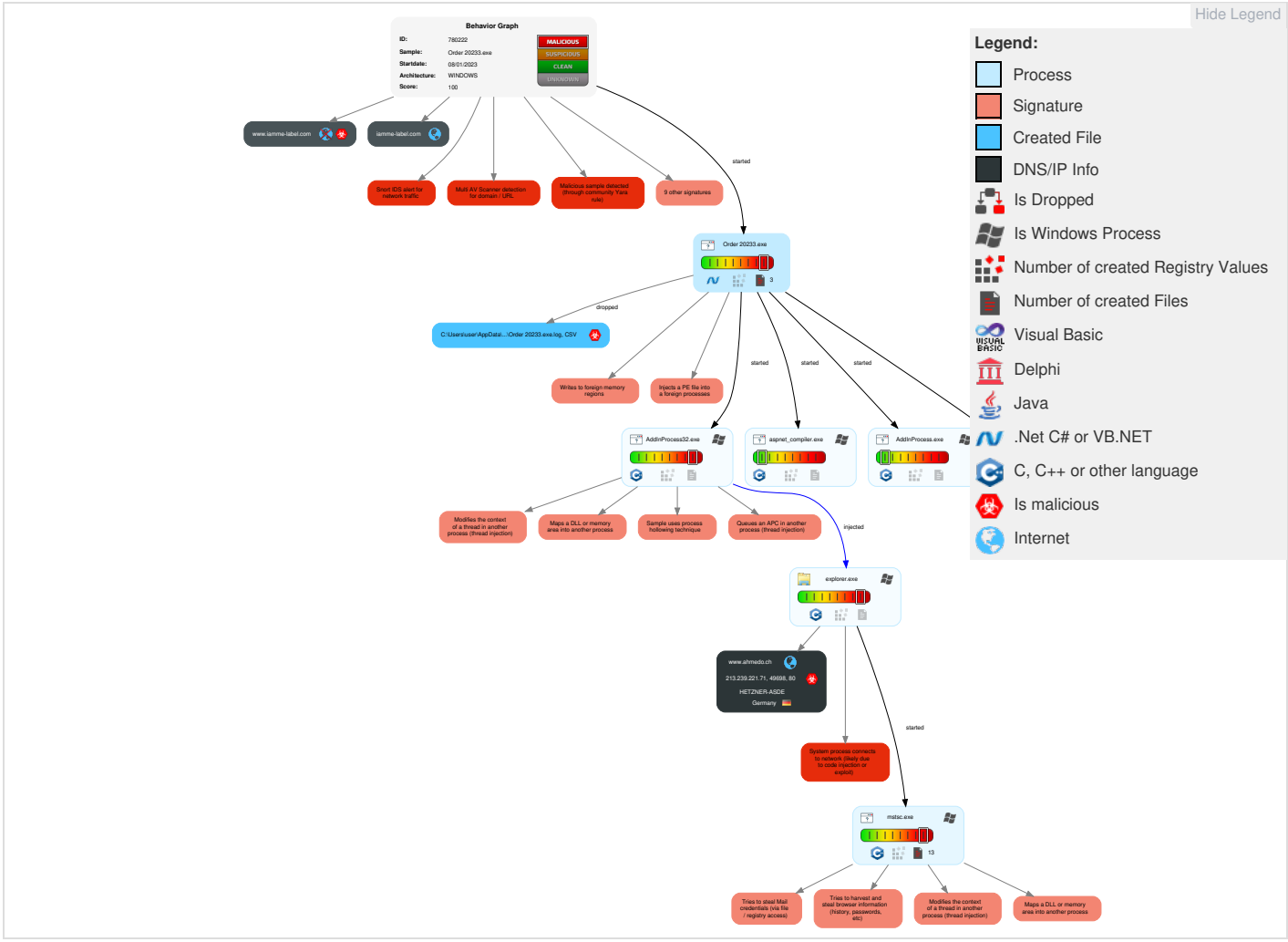
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	7 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	7 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
Order 20233.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	
Order 20233.exe	40%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.ahmedo.ch	4%	Virustotal		Browse
iamme-label.com	9%	Virustotal		Browse
www.iamme-label.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.sysinternals.com0	0%	URL Reputation	safe	
http://www.ahmedo.ch/dcn0/?pFQ0Q=4h6DHJsXwPiPeVap&oRk4IZo0=C4IpA5iiNFvhwRpGGB75QVE24l/FHjdcJi1XKvHDvYafZRhhpOblpVmnT5Y5r50LceSQqf3teF0eh20kxL606x8yuiPd0JQ74w==	100%	Avira URL Cloud	malware	
www.ahmedo.ch/dcn0/	10%	Virustotal		Browse
www.ahmedo.ch/dcn0/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ahmedo.ch	213.239.221.71	true	true	• 4%, Virustotal, Browse	unknown
iamme-label.com	81.169.145.80	true	false	• 9%, Virustotal, Browse	unknown
www.iamme-label.com	unknown	unknown	true	• 3%, Virustotal, Browse	unknown

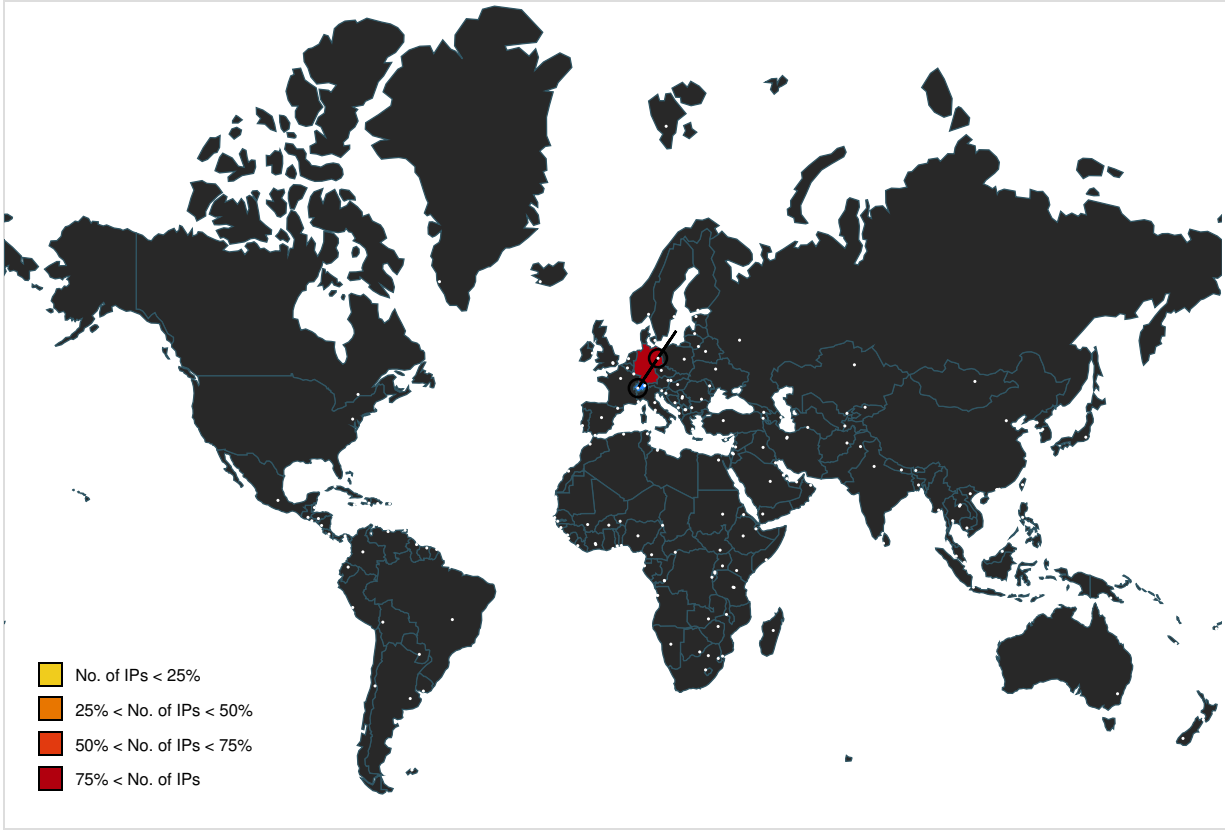
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.ahmedo.ch/dcn0/	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	low
http://www.ahmedo.ch/dcn0/?pFQ0Q=4h6DHJsXwPiPeVap&oRk4IZo0=C4IpA5iiNFvhwRpGGB75QVE24l/FHjdcJi1XKvHDvYafZRhhpOblpVmnT5Y5r50LceSQqf3teF0eh20kxL606x8yuiPd0JQ74w==	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	4184-48M.21.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	mstsc.exe, 00000015.00000003.521808734.000000001016000.00000004.00000020.00020000.00000000.sdmp, 4184-48M.21.dr	false		high
http://https://duckduckgo.com/chrome_newtab	mstsc.exe, 00000015.00000003.521808734.000000001016000.00000004.00000020.00020000.00000000.sdmp, 4184-48M.21.dr	false		high
http://https://duckduckgo.com/ac/?q=	4184-48M.21.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	mstsc.exe, 00000015.00000003.521808734.000000001016000.00000004.00000020.00020000.00000000.sdmp, 4184-48M.21.dr	false		high
http://https://www.sysinternals.com0	Order 20233.exe, 00000000.00000002.307240317.00000217000D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	mstsc.exe, 00000015.00000003.521808734.000000001016000.00000004.00000020.00020000.00000000.sdmp, 4184-48M.21.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	4184-48M.21.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	mstsc.exe, 00000015.00000003.521808734.000000001016000.00000004.00000020.00020000.00000000.sdmp, 4184-48M.21.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	4184-48M.21.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	mstsc.exe, 00000015.00000003.521808734.000000001016000.00000004.00000020.00020000.00000000.sdmp, 4184-48M.21.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.239.221.71	www.ahmedo.ch	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780222
Start date and time:	2023-01-08 16:21:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order 20233.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@22/2@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33.5% (good quality ratio 29.1%) • Quality average: 71.4% • Quality standard deviation: 33.6%

HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Order 20233.exe.log

Process:	C:\Users\user\Desktop\Order 20233.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	1510
Entropy (8bit):	5.381105762964764
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPN+84xpNT:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1f
MD5:	A3195731DF98BB6BDA4A3DE6D454C33C
SHA1:	CBEE1CB7EAFDE247618CC50DDE5D9A143732C7E4
SHA-256:	68DD8AFDE633D8CEF50498ADA0CAD19DEEAF370EB6A01D718D11A499D44E2CCA
SHA-512:	11DF23E67BBC8A6DA19406BB025FB0F90304B9FD7A2987FC7678E072AE288094A022E9BB8EDB06B102095BFB54BC8C703FD7D646925D6681F256B52354D04DFD

Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\AppData\Local\Temp\4184-48M	
Process:	C:\Windows\SysWOW64\mstsc.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.565938948299627
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	Order 20233.exe
File size:	1827328
MD5:	cfc3542e983b4a7436dabb73132cbbdb
SHA1:	c792d80b3667badeef358a872cc5b548d9114151
SHA256:	614490e3bf7cf0672ecda890e33b49f4f8b80da18333111489284df04ab7d934
SHA512:	f434b55379dc227f8908b6e25c39a61e699a0b6f90b5d48128f148c6c838ead6d8ec330191d62c409236bc109a95b7fa6a5ad234c99ee57584dc2405490d38fb
SSDEEP:	24576:0G/gSI7uzvdh53ATay0Lu9fE124K2Gzo/Xyhp4HtNLpTGLRvO4x:dgruLMayJWao/XC6B
TLSH:	258532203AFE601DF1B3AF795FF4759AA97FFA623B02945D1051034A0A23E41DDD1A3A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....L.Y....."...0..... ....@..... ....5.....` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59EE4CED [Mon Oct 23 20:11:25 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1c0000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1bfc02	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

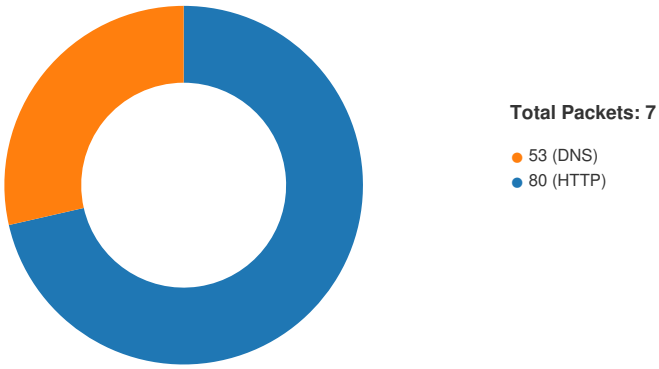
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1bdc8e	0x1bde00	False	0.39824640366554526	data	4.567184281741237	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x1c0000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3213.239.221.7 149698802031412 01/08/23-16:24:08.929621	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49698	80	192.168.2.3	213.239.221.71
192.168.2.3213.239.221.7 149698802031449 01/08/23-16:24:08.929621	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49698	80	192.168.2.3	213.239.221.71
192.168.2.3213.239.221.7 149698802031453 01/08/23-16:24:08.929621	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49698	80	192.168.2.3	213.239.221.71

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:24:08.907176018 CET	49698	80	192.168.2.3	213.239.221.71
Jan 8, 2023 16:24:08.929352045 CET	80	49698	213.239.221.71	192.168.2.3
Jan 8, 2023 16:24:08.929502010 CET	49698	80	192.168.2.3	213.239.221.71
Jan 8, 2023 16:24:08.929620981 CET	49698	80	192.168.2.3	213.239.221.71
Jan 8, 2023 16:24:08.952090025 CET	80	49698	213.239.221.71	192.168.2.3
Jan 8, 2023 16:24:08.957961082 CET	80	49698	213.239.221.71	192.168.2.3
Jan 8, 2023 16:24:08.958008051 CET	80	49698	213.239.221.71	192.168.2.3
Jan 8, 2023 16:24:08.958194971 CET	49698	80	192.168.2.3	213.239.221.71
Jan 8, 2023 16:24:08.958410025 CET	49698	80	192.168.2.3	213.239.221.71
Jan 8, 2023 16:24:08.980180025 CET	80	49698	213.239.221.71	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:24:08.849303961 CET	49977	53	192.168.2.3	8.8.8.8
Jan 8, 2023 16:24:08.895353079 CET	53	49977	8.8.8.8	192.168.2.3
Jan 8, 2023 16:24:18.985353947 CET	57840	53	192.168.2.3	8.8.8.8
Jan 8, 2023 16:24:19.005789042 CET	53	57840	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 8, 2023 16:24:08.849303961 CET	192.168.2.3	8.8.8.8	0x8412	Standard query (0)	www.ahmedo.ch	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:24:18.985353947 CET	192.168.2.3	8.8.8.8	0x2ac9	Standard query (0)	www.iamme-label.com	A (IP address)	IN (0x0001)	false

DNS Answers

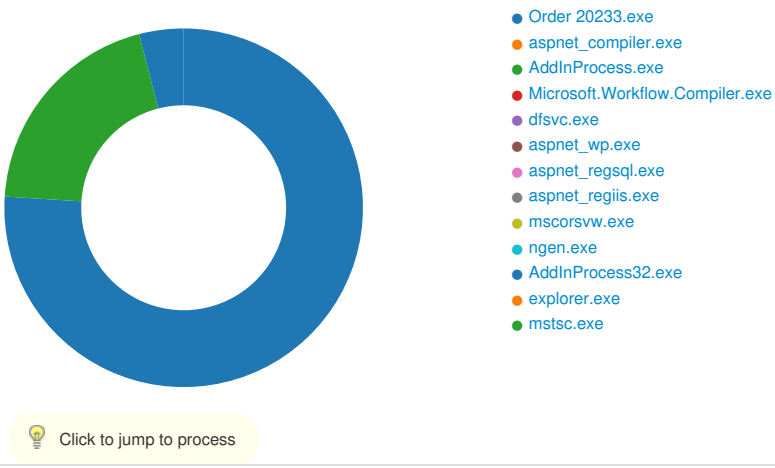
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:24:08.895353079 CET	8.8.8.8	192.168.2.3	0x8412	No error (0)	www.ahmedo.ch		213.239.221.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:24:19.005789042 CET	8.8.8.8	192.168.2.3	0x2ac9	No error (0)	www.iamme-label.com	iamme-label.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 8, 2023 16:24:19.005789042 CET	8.8.8.8	192.168.2.3	0x2ac9	No error (0)	iamme-label.com		81.169.145.80	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.ahmedo.ch

Statistics

Behavior



System Behavior

Analysis Process: Order 20233.exe PID: 5872, Parent PID: 3452

General

Target ID:	0
Start time:	16:23:10
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\Order 20233.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Order 20233.exe
Imagebase:	0x21772580000
File size:	1827328 bytes
MD5 hash:	CFC3542E983B4A7436DABB73132CBBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.307240317.00000217000D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

File Activities

Analysis Process: aspnet_compiler.exe PID: **6120**, Parent PID: **5872**

General	
Target ID:	4
Start time:	16:23:24
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x1eacc870000
File size:	54888 bytes
MD5 hash:	7809A19AA8DA1A41F36B60B0664C4E20
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: AddInProcess.exe PID: **2140**, Parent PID: **5872**

General	
Target ID:	6
Start time:	16:23:29
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess.exe
Imagebase:	0x1892c120000
File size:	42080 bytes
MD5 hash:	11D8A500C4C0FBAF20EBDB8CDF6EA452
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Microsoft.Workflow.Compiler.exe PID: **1360**, Parent PID: **5872**

General	
Target ID:	7
Start time:	16:23:29
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe
Imagebase:	0x29ba2ba0000
File size:	32872 bytes
MD5 hash:	D91462AE31562E241AF5595BA5E1A3C4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: dfsvc.exe PID: **2288**, Parent PID: **5872**

General	
Target ID:	8
Start time:	16:23:29
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\dfsvc.exe
Imagebase:	0x1be839a0000
File size:	24160 bytes
MD5 hash:	48FD4DD682051712E3E7757C525DED71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_wp.exe PID: **2104**, Parent PID: **5872**

General	
Target ID:	10
Start time:	16:23:30
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_wp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_wp.exe
Imagebase:	0x7ff651cf0000
File size:	50784 bytes
MD5 hash:	3F68BCF536EEAE067038C67022CDF6D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: aspnet_regsql.exe PID: **5300**, Parent PID: **5872**

General	
Target ID:	11
Start time:	16:23:30
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regsql.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regsql.exe
Imagebase:	0x15782f30000
File size:	126560 bytes
MD5 hash:	F31014EE4DE7FE48E9B7C9BE94CFB45F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: aspnet_regiis.exe PID: **1760**, Parent PID: **5872**

General	
Target ID:	13
Start time:	16:23:30

Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe
Imagebase:	0x7ff66ccd0000
File size:	44640 bytes
MD5 hash:	061D8C0371566D560C5B15C77A34046F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: mscorsvw.exe PID: **3956**, Parent PID: **5872**

General	
Target ID:	15
Start time:	16:23:31
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
Imagebase:	0x7ff7da510000
File size:	128584 bytes
MD5 hash:	B00E9325AC7356A3F4864EAAAD48E13F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ngen.exe PID: **5612**, Parent PID: **5872**

General	
Target ID:	16
Start time:	16:23:31
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe
Imagebase:	0x7ff63bfc0000
File size:	174184 bytes
MD5 hash:	FBA5E8D94C9EADC279BC06B9CF041A9A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: AddInProcess32.exe PID: **4392**, Parent PID: **5872**

General	
Target ID:	17
Start time:	16:23:31
Start date:	08/01/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
Imagebase:	0xe60000

File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000011.00000002.428209911.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.428209911.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000011.00000002.428209911.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.428209911.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.428209911.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000011.00000002.429045725.00000000017F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000011.00000002.429045725.00000000017F0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41DFAE	NtReadFile

Analysis Process: explorer.exe PID: 3452, Parent PID: 4392

General

Target ID:	20
Start time:	16:23:35
Start date:	08/01/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.374923978.000000001033E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000014.00000000.374923978.000000001033E000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.374923978.000000001033E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.374923978.000000001033E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mstsc.exe PID: 5380, Parent PID: 3452

General

Target ID:	21
Start time:	16:24:21
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x1310000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.531522475.00000000037F0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000015.00000002.524509054.0000000000BB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.524509054.0000000000BB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.524509054.0000000000BB0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.524509054.0000000000BB0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.524509054.0000000000BB0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000015.00000002.528604995.00000000012D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.528604995.00000000012D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.528604995.00000000012D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.528604995.00000000012D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.528604995.00000000012D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe	access denied	1	BCC8A7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\4184-48M	object name not found	1	BCC8A7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\4184-48M	sharing violation	1	BCC8A7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\4184-48M	sharing violation	1	BCC8A7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	BCC877	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly