ID: 532631
Sample Name: New Order4687334.exe
Cookbook: default.jbs
Time: 15:17:45
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

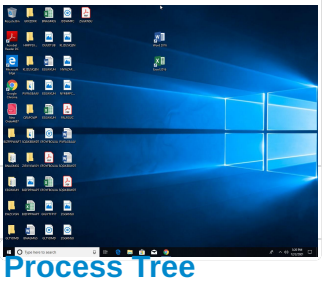
Windows Analysis Report New Order4687334.exe

Overview

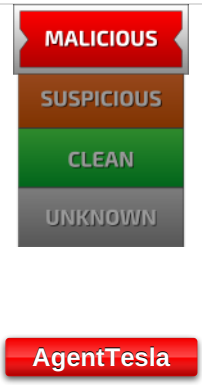
General Information

Sample Name:	New Order4687334.exe
Analysis ID:	532631
MD5:	abc0d5990e243c..
SHA1:	a62d9e6614ab92..
SHA256:	b8baaf727f8da89..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

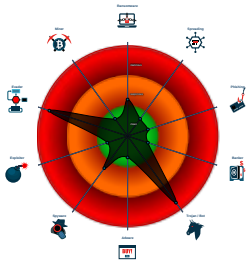


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Uses the Telegram API (likely for C&…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Sigma detected: Powershell Defende…

Classification



Process Tree

- **System is w10x64**
- New Order4687334.exe (PID: 4548 cmdline: "C:\Users\user\Desktop\New Order4687334.exe" MD5: ABC0D5990E243C73BCB0EF52F113C9C8)
  - powershell.exe (PID: 6580 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lGBqbwYsd.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 7064 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lGBqbwYsd" /XML "C:\Users\user\AppData\Local\Temp\tmp4E0D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - New Order4687334.exe (PID: 6184 cmdline: C:\Users\user\Desktop\New Order4687334.exe MD5: ABC0D5990E243C73BCB0EF52F113C9C8)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5074572303:AAE8ZKRzrDBFdUptPX0s5TohA3XJtaS_H_8/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1898999986",
  "Chat URL": "https://api.telegram.org/bot5074572303:AAE8ZKRzrDBFdUptPX0s5TohA3XJtaS_H_8/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.529256837.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.529256837.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000F.00000000.311913229.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000000.311913229.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.316046595.000000000326 7000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.New Order4687334.exe.41e0718.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.New Order4687334.exe.41e0718.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.New Order4687334.exe.4216938.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.New Order4687334.exe.4216938.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.New Order4687334.exe.4216938.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

Uses the Telegram API (likely for C&C communication)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality:

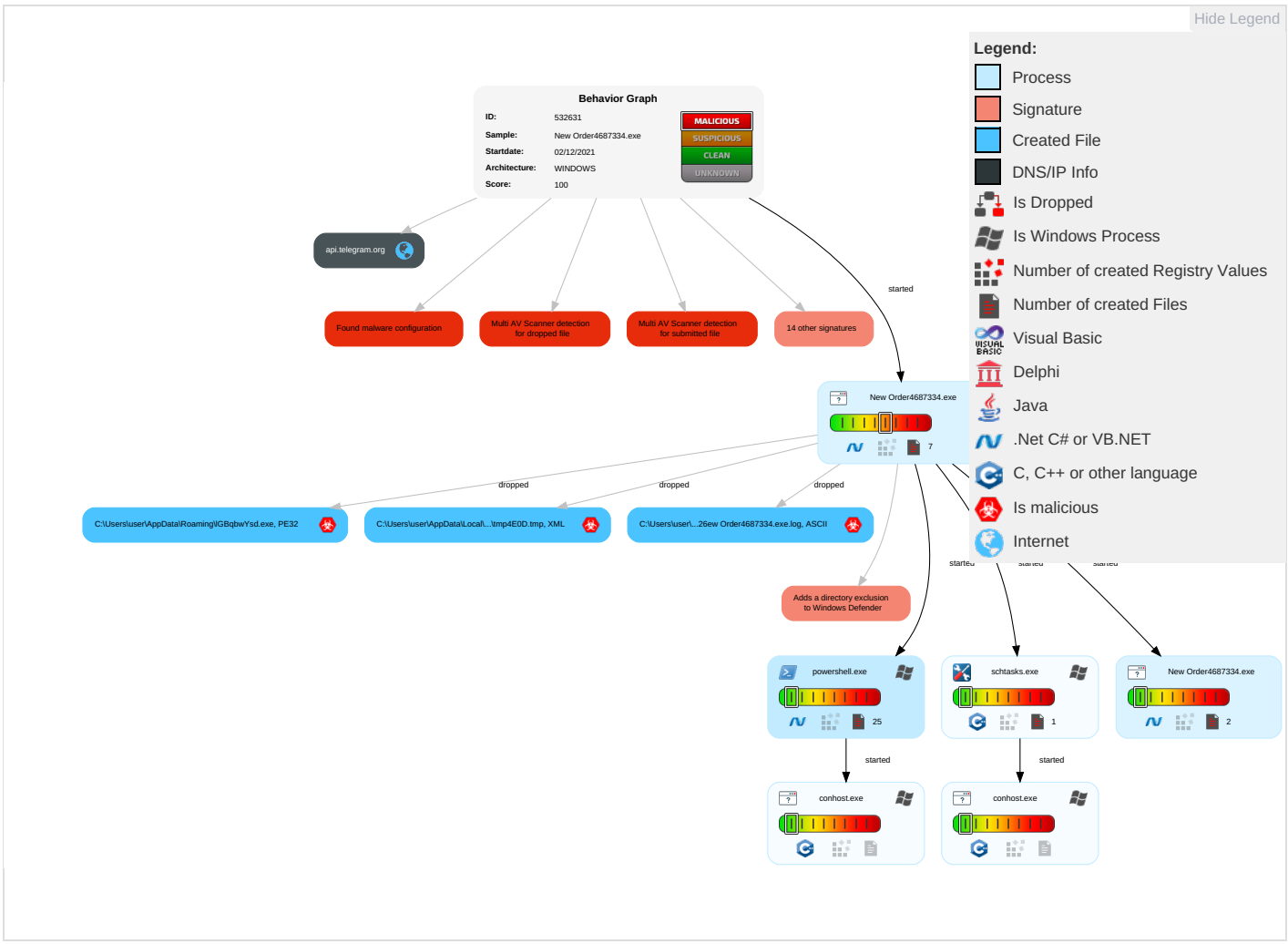
Yara detected Telegram RAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1	Eav Inse Net Con
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 3 1 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exp Red Call
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exp Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Con
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc

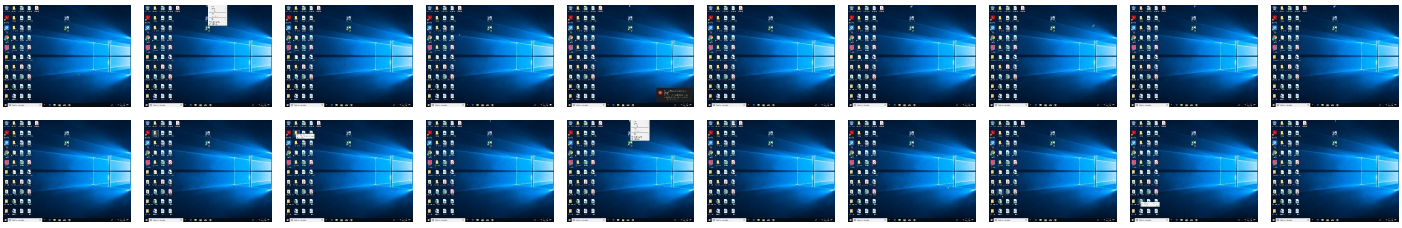
Behavior Graph



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 Order4687334.exe	41%	Virustotal		Browse
New Order4687334.exe	38%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lGBqbwYsd.exe	38%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.New Order4687334.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.New Order4687334.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.2.New Order4687334.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.New Order4687334.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.New Order4687334.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.New Order4687334.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

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://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://psZqXY.com	2%	Virustotal		Browse
http://psZqXY.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.telegram.orgD8ol	0%	Avira URL Cloud	safe	
http://xd9ilaiS4bffM0SeD.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.telegram.org4ol	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532631
Start date:	02.12.2021
Start time:	15:17:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order4687334.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:	28
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@9/8@1/0
EGA Information:	Failed
HDC Information:	Failed

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

Simulations

Behavior and APIs

Time	Type	Description
15:18:52	API Interceptor	603x Sleep call for process: New Order4687334.exe modified
15:19:06	API Interceptor	27x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	SWIFT_ADVICE.exe	Get hash	malicious	Browse	• 149.154.167.220
	Overdue outstanding payment.exe	Get hash	malicious	Browse	• 149.154.167.220
	proforma invoice packing list.exe	Get hash	malicious	Browse	• 149.154.167.220
	KG236KQE0b.exe	Get hash	malicious	Browse	• 149.154.167.220
	TT COPY.exe	Get hash	malicious	Browse	• 149.154.167.220
	Invoice.doc.scr.exe	Get hash	malicious	Browse	• 149.154.167.220
	proforma invoice packing list.exe	Get hash	malicious	Browse	• 149.154.167.220
	PROFORMA.EXE	Get hash	malicious	Browse	• 149.154.167.220
	Proforma-Invoice CAC1105 CI&PL.exe	Get hash	malicious	Browse	• 149.154.167.220
	8VVKoakLYt.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.GenericKD.47502835.19614.exe	Get hash	malicious	Browse	• 149.154.167.220
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 149.154.167.220
	Quote.exe	Get hash	malicious	Browse	• 149.154.167.220
	Dhl delivery Express.exe	Get hash	malicious	Browse	• 149.154.167.220
	stampa_CFS-ITALIA_1123311-655.exe	Get hash	malicious	Browse	• 149.154.167.220
	Launcher.exe	Get hash	malicious	Browse	• 149.154.167.220
	BANKASI 657090031.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Variant.Barys.226418.1879.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Trojan.GenericKD.38103794.11009.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.SpyBot.1125.26781.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order4687334.exe.log	
Process:	C:\Users\user\Desktop\New Order4687334.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22296
Entropy (8bit):	5.604691119582736
Encrypted:	false
SSDEEP:	384:ut3Gy/SQjpTZLtSBKnYjultI+3uB9gPSJ3x+T1M4/ZlbAV7HQWDa5ZBDI+i6Yz:xGZJ4KYCltB3PcsCwfwDCVO
MD5:	A4ED3D527A314AF2DF3B2F6646512FC2
SHA1:	118D9F6F19D634E54694199804A68C4BE8BF0516
SHA-256:	B35E5F9892334A2B86B02C5A779AFA465AB7857BBD37D3A6A9F06939F23A11A2
SHA-512:	4758E7B471FF90F37010FE776F0B20E012257005FBFDF8BA0FF465E30C5E8C4517E1E04B6A5BC6B6956420326C4B7114DCE65573AB27C8B9BCD8901002E6F022
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h...h.d.a.....&. .H.....@.....H.....<@.^.L."My...:?..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..4.....].D.E.....#.....System.Data.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServicesH..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mphuq2tu.k3a.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mphuq2tu.k3a.ps1	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yxf2igxg.heq.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp4E0D.tmp	
Process:	C:\Users\user\Desktop\New Order4687334.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	5.136404201143362
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtyhxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTynv
MD5:	AFDE0ABCE5DACF961010261FC91DA9D3
SHA1:	DE619D02A4142F3C96B551B4316B7573A003355C
SHA-256:	12B2F1266A20D8445BE2D61BB191C85CD39BF557D624D7CAAA1C025A1FF82FAD
SHA-512:	878CA3E22C23DCDC8286C19A70018ADBD2D8963F023600870DD9566D0BDDA436786F1495C95A68292C5BB2C1C176A81296D8DD016BCEC1912ACC00671DB23DF
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvai

C:\Users\user\AppData\Roaming\lGBqbwYsd.exe	
Process:	C:\Users\user\Desktop\New Order4687334.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	811008
Entropy (8bit):	7.627401226270159
Encrypted:	false
SSDEEP:	24576:+MjgD5aplp3dWwft/4kCO9MR3MByLZKb6:58YplrWO9O3MBAK
MD5:	ABC0D5990E243C73BCB0EF52F113C9C8
SHA1:	A62D9E6614AB925A6EC5EC1D8C8ABEB44CF51EF0
SHA-256:	B8BAAF727F8DA89FE81122FD5C93C3D34B7F3F78AE90403309D7D335E0BB3792

C:\Users\user\AppData\Roaming\lGBqbwYsd.exe	
SHA-512:	C33CDB17D07AF0B51B4DFDF1A4626EC94AD87D24AEF2E4AC8CC17EECDFDFE246224A28E448D321FEB4EA70D83A349F822ED46ABAD7EC1913566B83A2C9BC4FA5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*.a.....0.....>.... .....@.. ....@.....O..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....^.....@..B..... .....H.....p>...F.....Z.....f.....0..7.....=...%....r...p.....%.r...p.%.r...p.%...(.....+..*".(.....*&.(.....**..(.....*....(.....*.... (.....*....0.....d.....{.....o.....+..*....0..3.....{....s.....o.....(I.....,..r#..psO...z..}....*..0.....o.....0..o.....0..o.....2..o.....+.....,..r...pr...ps....z.o.....o....ZX..{.....,..r...ps.. ..z..{....o.....+_..(.....oL.....,B..{.....s/..

C:\Users\user\AppData\Roaming\lGBqbwYsd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\New Order4687334.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211202\PowerShell_transcript.830021.Zh+Xk+NK.20211202151904.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5825
Entropy (8bit):	5.39302879110607
Encrypted:	false
SSDEEP:	96:BZd6KNSUqDo1ZKZAd6KNSUqDo1ZbVPNjZAd6KNSUqDo1ZbkddUZ/:OOqfq0
MD5:	52A4E973959AE0EC62F760F9857FA139
SHA1:	1ABBBD65F5D536E9F1F5A8F491E8D8AEC47ADEDF
SHA-256:	85A95B5DAC66490EA7AFE6BA7F250FA44D233B63167CDEED5C509F304BECD2F2
SHA-512:	69F9CFEB22E0824AD47FD5E1B5F0CB7D6ACD48239927C68EDB2E4E02AA4989CC80586545B82CC00FDABFDE5E2D3792AA366DA4AF8FA4DA5F897800DC07B6618
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202151906..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lGBqbwYsd.exe..Process ID: 6580..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211202151906..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lGBqbwYsd.exe..**********..Windows PowerShell transcript start..Start time: 20211202152227..Username: computer\user..RunAs User: DE

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.627401226270159
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	New Order4687334.exe
File size:	811008
MD5:	abc0d5990e243c73bcb0ef52f113c9c8
SHA1:	a62d9e6614ab925a6ec5ec1d8c8abeb44cf51ef0

General

SHA256:	b8baaf727f8da89fe81122fd5c93c3d34b7f3f78ae90403309d7d335e0bb3792
SHA512:	c33cdb17d07af0b51b4dfdf1a4626ec94ad87d24aef2e4ac8cc17eecdfdfe246224a28e448d321feb4ea70d83a349f822ed46abad7ec1913566b83a2c9bc4fa5
SSDEEP:	24576:+MjgD5aplp3dWwft/4kCO9MR3MByLZKb6:58YplrWO9O3MBAK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*.a.....0.....>.... .....@.. .....@.....

File Icon

Icon Hash:	ce9ab2a29a9aa2d4

Static PE Info

General

Entrypoint:	0x4aec3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A82ACB [Thu Dec 2 02:09:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xacc44	0xace00	False	0.917266867769	data	7.85496996134	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x18ce0	0x18e00	False	0.112535332915	data	4.31172980931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:20:56.626312971 CET	192.168.2.7	8.8.8.8	0x623f	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

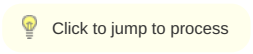
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:20:56.646023989 CET	8.8.8.8	192.168.2.7	0x623f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New Order4687334.exe PID: 4548 Parent PID: 6072

General

Start time:	15:18:51
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\New Order4687334.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\New Order4687334.exe"
Imagebase:	0x7ff641cd0000
File size:	811008 bytes
MD5 hash:	ABC0D5990E243C73BCB0EF52F113C9C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.316046595.0000000003267000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.318200591.00000000040BF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.318200591.00000000040BF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.315258817.0000000002FA1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6580 Parent PID: 4548

General

Start time:	15:19:03
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lGBqbwYsd.exe
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6732 Parent PID: 6580

General

Start time:	15:19:03
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: schtasks.exe PID: 7064 Parent PID: 4548

General

Start time:	15:19:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lGBqbwYsd" /XML "C:\Users\user\AppData\Local\Temp\tmp4E0D.tmp
Imagebase:	0x1120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 7132 Parent PID: 7064

General

Start time:	15:19:10
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: New Order4687334.exe PID: 6184 Parent PID: 4548

General

Start time:	15:19:12
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\New Order4687334.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New Order4687334.exe
Imagebase:	0xb10000
File size:	811008 bytes
MD5 hash:	ABC0D5990E243C73BCB0EF52F113C9C8
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: 0000000F.00000002.529256837.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.529256837.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.311913229.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.311913229.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.310261414.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.310261414.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.534092510.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000F.00000002.534092510.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.534092510.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.311127679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.311127679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.312585278.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.312585278.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis