ID: 323002
Sample Name: New PO 64739 (UK).exe
Cookbook: default.jbs
Time: 07:56:59
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

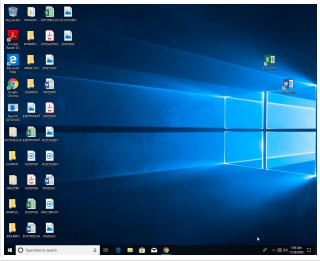
Analysis Report New PO 64739 (UK).exe

Overview

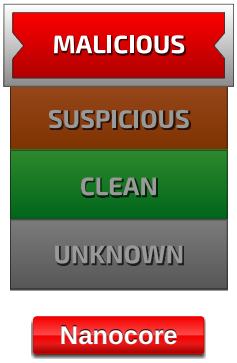
General Information

Sample Name:	New PO 64739 (UK).exe
Analysis ID:	323002
MD5:	b6babb0d3661cd..
SHA1:	de2db850207d77..
SHA256:	bca89f6ecbf4dfd…
Tags:	NanoCore

Most interesting Screenshot:



Detection

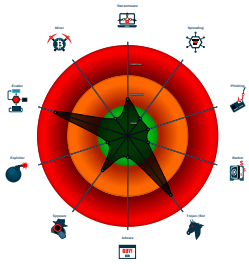


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…
- Uses schtasks.exe or at.exe to add …
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- New PO 64739 (UK).exe (PID: 1308 cmdline: 'C:\Users\user\Desktop\New PO 64739 (UK).exe' MD5: B6BABB0D3661CD172C93C496DC4C1DB1)
  - schtasks.exe (PID: 5904 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TqGgKBQek' /XML 'C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6016 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "185.140.53.207"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.509333754.0000000003F73000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.510190949.0000000004B1F000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.510190949.0000000004B1F000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x15f1:$a: NanoCore • 0x164a:$a: NanoCore • 0x1687:$a: NanoCore • 0x1700:$a: NanoCore • 0x14dab:$a: NanoCore • 0x14dc0:$a: NanoCore • 0x14df5:$a: NanoCore • 0x22a0a:$a: NanoCore • 0x22a2f:$a: NanoCore • 0x22a88:$a: NanoCore • 0x32c25:$a: NanoCore • 0x32c4b:$a: NanoCore • 0x32ca7:$a: NanoCore • 0x3fafc:$a: NanoCore • 0x3fb55:$a: NanoCore • 0x3fb88:$a: NanoCore • 0x3fdb4:$a: NanoCore • 0x3fe30:$a: NanoCore • 0x40449:$a: NanoCore • 0x40592:$a: NanoCore • 0x40a66:$a: NanoCore
00000004.00000002.502584081.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.502584081.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.MSBuild.exe.55c0000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
4.2.MSBuild.exe.55c0000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
4.2.MSBuild.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4.2.MSBuild.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
4.2.MSBuild.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 1 entries				

Sigma Overview

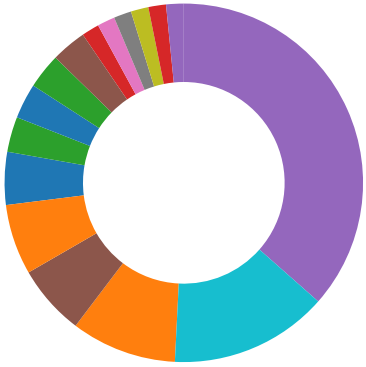
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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 AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

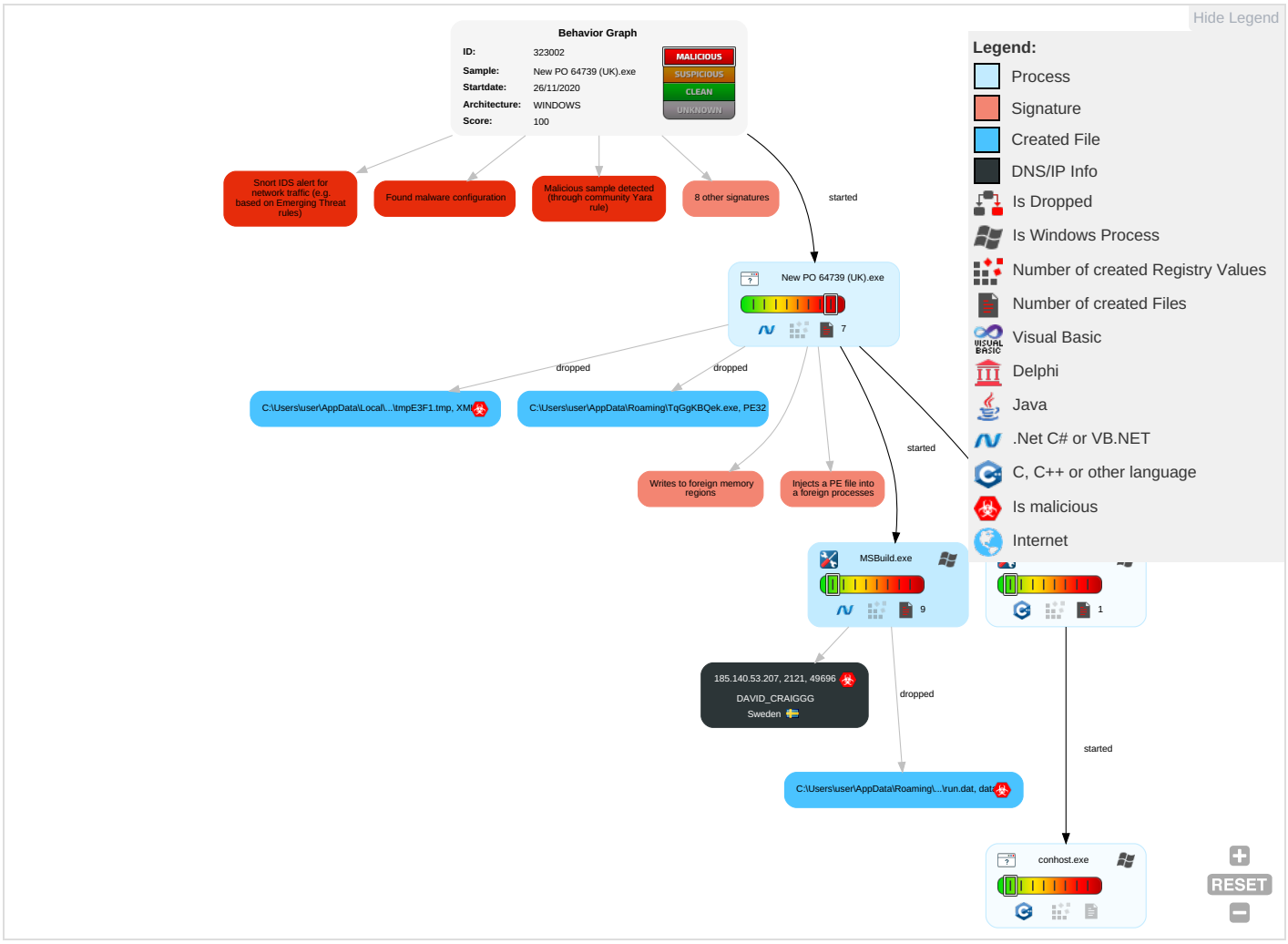
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 1	Input Capture 2 1	Security Software Discovery 1 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E I N C
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

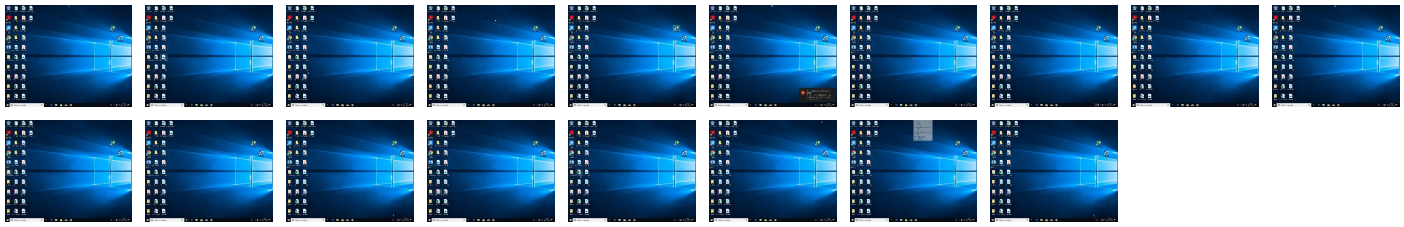
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	New PO 64739 (UK).exe, 0000000 0.00000002.265011054.000000000 32E1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.207	unknown	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323002
Start date:	26.11.2020
Start time:	07:56:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New PO 64739 (UK).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:	15
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@6/8@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.3%) • Quality average: 52.8% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 98% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 40.88.32.150, 92.122.144.200, 13.88.21.125, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, fs.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/323002/sample/New PO 64739 (UK).exe

Simulations

Behavior and APIs

Time	Type	Description
07:58:00	API Interceptor	1x Sleep call for process: New PO 64739 (UK).exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.207	DHL ShipmentDHL Shipment 237590.pdf.exe	Get hash	malicious	Browse	
	Doc_AWB#5305323204643_UPS.pdf.exe	Get hash	malicious	Browse	
	irs Doc Attached.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	90987948.exe	Get hash	malicious	Browse	• 185.244.30.223
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 185.140.53.149
	PO456789.exe	Get hash	malicious	Browse	• 185.244.30.212
	kelvinx.exe	Get hash	malicious	Browse	• 185.140.53.132
	Order-2311.exe	Get hash	malicious	Browse	• 91.193.75.147
	YZD221120.exe	Get hash	malicious	Browse	• 91.193.75.147
	ORDER #201120A.exe	Get hash	malicious	Browse	• 185.244.30.92
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 185.140.53.149
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Ups file de.exe	Get hash	malicious	Browse	• 185.140.53.221
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 185.140.53.149
	purchase order.exe	Get hash	malicious	Browse	• 185.140.53.233
	Remittance Details.xls	Get hash	malicious	Browse	• 185.140.53.184
	PaymentConfirmation.exe	Get hash	malicious	Browse	• 185.140.53.183
	ORDER #02676.doc.exe	Get hash	malicious	Browse	• 185.244.30.92
	b11305c6ab207f830062f80eeec728c4.exe	Get hash	malicious	Browse	• 185.140.53.233
	ShippingDoc.jar	Get hash	malicious	Browse	• 185.244.30.139
	1kn1ejwPxi.exe	Get hash	malicious	Browse	• 185.140.53.132
	D6vy84l7rJ.exe	Get hash	malicious	Browse	• 185.140.53.149

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New PO 64739 (UK).exe.log	
Process:	C:\Users\user\Desktop\New PO 64739 (UK).exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C58018934011086A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New PO 64739 (UK).exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp	
Process:	C:\Users\user\Desktop\New PO 64739 (UK).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.175965126269107
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3Q
MD5:	40116A05B516A07CF1C194259F56F2D2
SHA1:	8A86389C92C0A7C9E6CF5467E15CFF7BC9750142
SHA-256:	F7BCDA8DF5E89517F99B4E4AC8CD5FAF36A9AEEB5B39DDAF753AADFD7FEDAC69
SHA-512:	4A9ED1686A93C54A5B3BB3193FEAF1EC322760876EB0A210A9D8734B886A7A7AEFD657B750271C5966CDFB98358D01730385ED5653994BE39685CD2BA992B8E
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:fLNt:fLNt
MD5:	78D38F5EA0447F24368720C617A73787
SHA1:	40D69D1741E9DFCE88591F7D9E536742746EB82D
SHA-256:	5BF50106AF31E263A4E0286B8B0B3E2ACCAA5BFFF07418A5756C632FE62748D8
SHA-512:	17192164B2C28B723F1187071B737B97C780F9CB3424CDFCEB063FEA1F38BD3377F3424F8AA3B9A1F4F0090A95D45084A6F1306DEB1BAEDA453C4D7978690343
Malicious:	**true**
Preview:	W...$..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.''''.v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\TqGgKBQek.exe	
Process:	C:\Users\user\Desktop\New PO 64739 (UK).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	936960
Entropy (8bit):	7.261816231890523
Encrypted:	false
SSDEEP:	12288:zpH4EQ1NXT5zPvEzOh3CqA5vLs1R5eyZIHCJL4SI571xTXcsPPQk3LPf0TzAH8Uh:zpH4EQj5LvEKoq+vk2y6iJL4/ZcoPQa
MD5:	B6BABB0D3661CD172C93C496DC4C1DB1
SHA1:	DE2DB850207D77611F557A060681F2C2A19AE1EF
SHA-256:	BCA89F6ECBF4DFDE0CC003B96F907AE1AB9B33A64650836D547D07291A059E86
SHA-512:	45DCE5171772DB72BF71FC72DAB6FEDA73995E7009F6B0BB74B2F25D6A5E23284C06C167505D56C79C6334A6E14E2B44B3117A4207F4396D4F71F01B1381CE91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..@.....^_... ...`....@.. ..... ..@.....\_..W....`..... ....H.....text...d?... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....J.....@..B.....@_.....H.....1....r...i.....0.....(....*...0..X.....r...p. .u.. ..A.a%...^E.....a.....Q.....8....r...p (..... ..Z ..B.a+..(....(....r...p(...., .i..%+. .1.%&.]...Za8w...(..... ..}.8g....r...p(....(...., z-.%+. >1..%&. ".@.Za89....-. ...m%+. <..?%&. ..HZa8.....(.... .Ej.8.....s....(....%.(.....(.... . -.8.....r;..p(....(....-. ..X.%+. ....%&. ...Za8....*.0.....('...*..0..y...

C:\Users\user\AppData\Roaming\TqGgKBQek.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\New PO 64739 (UK).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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.261816231890523
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	New PO 64739 (UK).exe
File size:	936960
MD5:	b6babb0d3661cd172c93c496dc4c1db1
SHA1:	de2db850207d77611f557a060681f2c2a19ae1ef
SHA256:	bca89f6ecbf4dfde0cc003b96f907ae1ab9b33a64650836d547d07291a059e86
SHA512:	45dce5171772db72bf71fc72dab6feda73995e7009f6b0bb74b2f25d6a5e23284c06c167505d56c79c6334a6e14e2b44b3117a4207f4396d4f71f01b1381ce91
SSDEEP:	12288:zpH4EQ1NXT5zPvEzOh3CqA5vLs1R5eyZIHCJL4Sl571xTXcsPPQk3LPf0TzAH8Uh:zpH4EQj5LvEKoq+vk2y6iJL4/ZcoPQa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..@.....^_... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e5f5e
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:	0x5FBF0D88 [Thu Nov 26 02:06:00 2020 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

Instruction
jmp dword ptr [00402000h]
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
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

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 al, byte ptr [eax]
adc byte ptr [eax], al
add byte ptr [eax], al
and byte ptr [eax], al
add byte ptr [eax+00000018h], al
push eax
add byte ptr [eax], al
add byte ptr [eax], 00000000h
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	0xe5f04	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe6000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe3f64	0xe4000	False	0.677923905222	data	7.26752340009	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x610	0x800	False	0.33203125	data	3.44745876984	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe60a0	0x380	data		
RT_MANIFEST	0xe6420	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

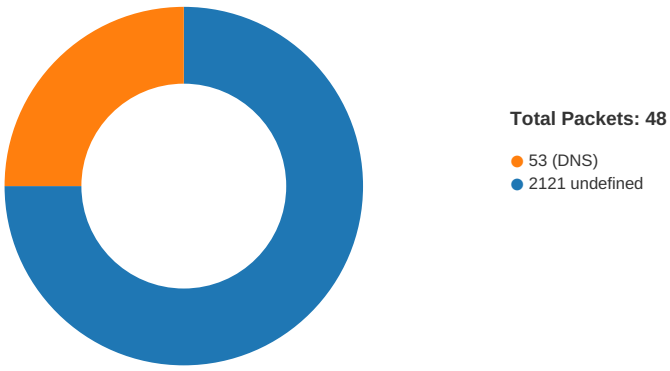
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2017
Assembly Version	1.0.0.0
InternalName	D0I8.exe
FileVersion	1.0.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	Arizona Lottery Numbers
ProductVersion	1.0.0.0
FileDescription	Arizona Lottery Numbers
OriginalFilename	D0I8.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-07:58:09.962435	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	2121	192.168.2.5	185.140.53.207

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 07:58:09.412566900 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:09.600203037 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:09.601804018 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:09.962435007 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:10.194097042 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:10.194221973 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:10.330408096 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:10.374310017 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:10.474917889 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:10.476288080 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:10.672211885 CET	2121	49696	185.140.53.207	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 07:58:10.730436087 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:11.590236902 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:11.832217932 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.900038004 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.911977053 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.912074089 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:11.923166990 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.949445963 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.949527025 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:11.957570076 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.958695889 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.958776951 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:11.963496923 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.977087975 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.977183104 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:11.984600067 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.986860991 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:11.986922979 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.133230925 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.140045881 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.140134096 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.142187119 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.150316954 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.150433064 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.158349037 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.180748940 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.180825949 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.184549093 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.188622952 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.188694954 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.192312002 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.196543932 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.196631908 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.216207027 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.220406055 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.220484972 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.227711916 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.240216970 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.240300894 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.248502970 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.252180099 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.252219915 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.252269030 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.256283998 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.256361961 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.262342930 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.268275023 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.268388987 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.318229914 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.324033022 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.324158907 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.330143929 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.334355116 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.334450960 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.340353012 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.346663952 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.346822977 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.350425959 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.354381084 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.354475021 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.380394936 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.400417089 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.400449991 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.400563955 CET	49696	2121	192.168.2.5	185.140.53.207

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 07:58:12.408484936 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.408616066 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.412388086 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.412720919 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.412800074 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.414218903 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.434391975 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.434525013 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.438570023 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.442373991 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.442477942 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.442569971 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.448462009 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.448563099 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.450156927 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.456665039 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.456789970 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.478627920 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.478655100 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.478744984 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.486334085 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.486361980 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.486494064 CET	49696	2121	192.168.2.5	185.140.53.207
Nov 26, 2020 07:58:12.488359928 CET	2121	49696	185.140.53.207	192.168.2.5
Nov 26, 2020 07:58:12.510396957 CET	2121	49696	185.140.53.207	192.168.2.5

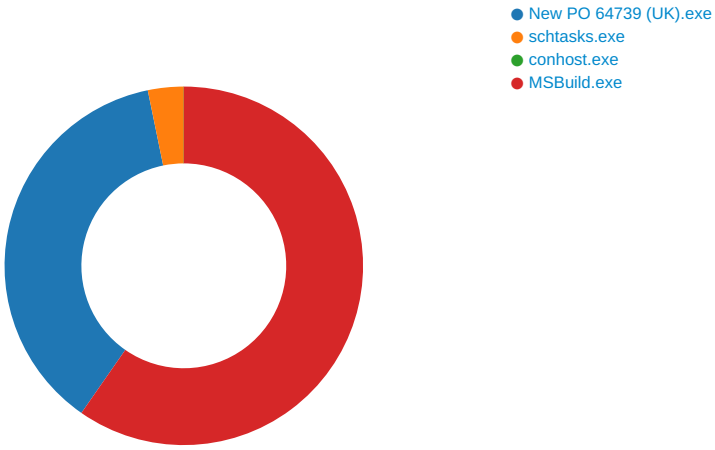
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 07:57:57.998034954 CET	64936	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:57:58.033602953 CET	53	64936	8.8.8.8	192.168.2.5
Nov 26, 2020 07:57:58.863831997 CET	52704	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:57:58.899288893 CET	53	52704	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:01.444466114 CET	52212	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:01.471843958 CET	53	52212	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:07.016284943 CET	54302	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:07.053309917 CET	53	54302	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:33.139759064 CET	53784	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:33.166909933 CET	53	53784	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:33.970594883 CET	65307	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:33.998008966 CET	53	65307	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:38.145914078 CET	64344	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:38.185548067 CET	53	64344	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:40.843112946 CET	62060	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:40.870227098 CET	53	62060	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:41.683815002 CET	61805	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:41.711005926 CET	53	61805	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:42.546552896 CET	54795	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:42.573625088 CET	53	54795	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:43.389050007 CET	49557	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:43.416213989 CET	53	49557	8.8.8.8	192.168.2.5
Nov 26, 2020 07:58:44.212383032 CET	61733	53	192.168.2.5	8.8.8.8
Nov 26, 2020 07:58:44.239660978 CET	53	61733	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New PO 64739 (UK).exe PID: 1308 Parent PID: 5628

General

Start time:	07:57:53
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\New PO 64739 (UK).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New PO 64739 (UK).exe'
Imagebase:	0xf40000
File size:	936960 bytes
MD5 hash:	B6BABB0D3661CD172C93C496DC4C1DB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.265011054.00000000032E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.266893873.00000000042E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.266893873.00000000042E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.266893873.00000000042E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.267084624.0000000004332000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.267084624.0000000004332000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.267084624.0000000004332000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.265117190.0000000003390000.00000004.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Roaming\TqGgKBQek.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C90DD66	CopyFileW
C:\Users\user\AppData\Roaming\TqGgKBQek.exe\:Zone.Identifier :$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C90DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New PO 64739 (UK).exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp	success or wait	1	6C906A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\TqGgKBQek.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 88 0d bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 40 0e 00 00 0a 00 00 00 00 00 00 5e 5f 0e 00 00 20 00 00 00 60 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P..@..........^_... ...`.. ..@.. ....@.................	success or wait	4	6C90DD66	CopyFileW
C:\Users\user\AppData\Roaming\TqGgKBQek.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C90DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New PO 64739 (UK).exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"Microsoft.VisualBasic, Ver	success or wait	1	6DDCC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: schtasks.exe PID: 5904 Parent PID: 1308

General

Start time:	07:58:04
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TqGgKBQek' /XML 'C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp'
Imagebase:	0x860000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp	unknown	2	success or wait	1	86AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE3F1.tmp	unknown	1647	success or wait	1	86ABD9	ReadFile

Analysis Process: conhost.exe PID: 5900 Parent PID: 5904

General

Start time:	07:58:05
Start date:	26/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: MSBuild.exe PID: 6016 Parent PID: 1308

General

Start time:	07:58:05
Start date:	26/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0xbb0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.509333754.0000000003F73000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.510190949.0000000004B1F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.510190949.0000000004B1F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.502584081.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.502584081.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.502584081.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.505217823.0000000002F21000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.509509822.00000000047EE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.505295151.0000000002F8C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.510056845.0000000004A34000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.509942877.00000000049FA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.512849217.00000000055C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.512849217.00000000055C0000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

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	6DABCF06	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	6DABCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C90BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	57 11 fa 10 24 92 d8 48	W...$..H	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	6C901B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C901B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DA9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	4096	success or wait	1	6DA7D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	unknown	512	success or wait	1	6DA7D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DA95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DA95705	unknown

Disassembly

Code Analysis