ID: 526564
Sample Name: PO-139178905466534553452009 14.PDF.EXE
Cookbook: default.jbs
Time: 18:53:36
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

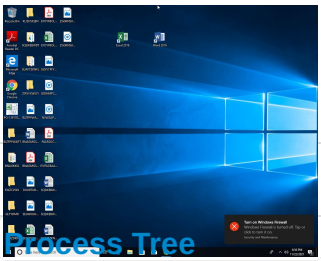
Windows Analysis Report PO-139178905466534553452009…

Overview

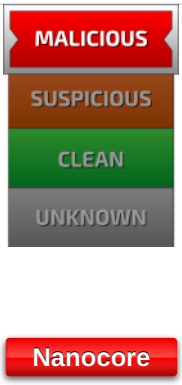
General Information

Sample Name:	PO-139178905466534553452009 14.PDF.EXE
Analysis ID:	526564
MD5:	84449b1242cb54..
SHA1:	5e652729685a27..
SHA256:	2b8acfa28705c83..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

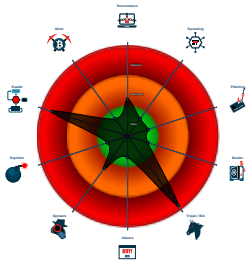


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for samp…

Classification



- **System is w10x64**
- PO-139178905466534553452009 14.PDF.EXE (PID: 5672 cmdline: "C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE" MD5: 84449B1242CB54AFC4BB3E9B628FDFAC)
  - powershell.exe (PID: 2892 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5320 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JlUFSgJsk.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1760 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JlUFSgJsk" /XML "C:\Users\user\AppData\Local\Temp\tmpC2D8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6532 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "1d5c6a3e-60c1-4684-aee7-fbdc0338",
  "Domain1": "185.157.160.229",
  "Domain2": "neoncorex.duckdns.org",
  "Port": 60006,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.321914533.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000000.321914533.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000000.321914533.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000A.00000002.557435379.0000000003CC9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.557435379.0000000003CC9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f45:$a: NanoCore • 0x2f9e:$a: NanoCore • 0x2fdb:$a: NanoCore • 0x3054:$a: NanoCore • 0x166ff:$a: NanoCore • 0x16714:$a: NanoCore • 0x16749:$a: NanoCore • 0x2f1d3:$a: NanoCore • 0x2f1e8:$a: NanoCore • 0x2f21d:$a: NanoCore • 0x2fa7:$b: ClientPlugin • 0x2fe4:$b: ClientPlugin • 0x38e2:$b: ClientPlugin • 0x38ef:$b: ClientPlugin • 0x164bb:$b: ClientPlugin • 0x164d6:$b: ClientPlugin • 0x16506:$b: ClientPlugin • 0x1671d:$b: ClientPlugin • 0x16752:$b: ClientPlugin • 0x2ef8f:$b: ClientPlugin • 0x2efaa:$b: ClientPlugin
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.MSBuild.exe.55f0000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
10.2.MSBuild.exe.55f0000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
10.2.MSBuild.exe.5750000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
10.2.MSBuild.exe.5750000.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
10.2.MSBuild.exe.5750000.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 60 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

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

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

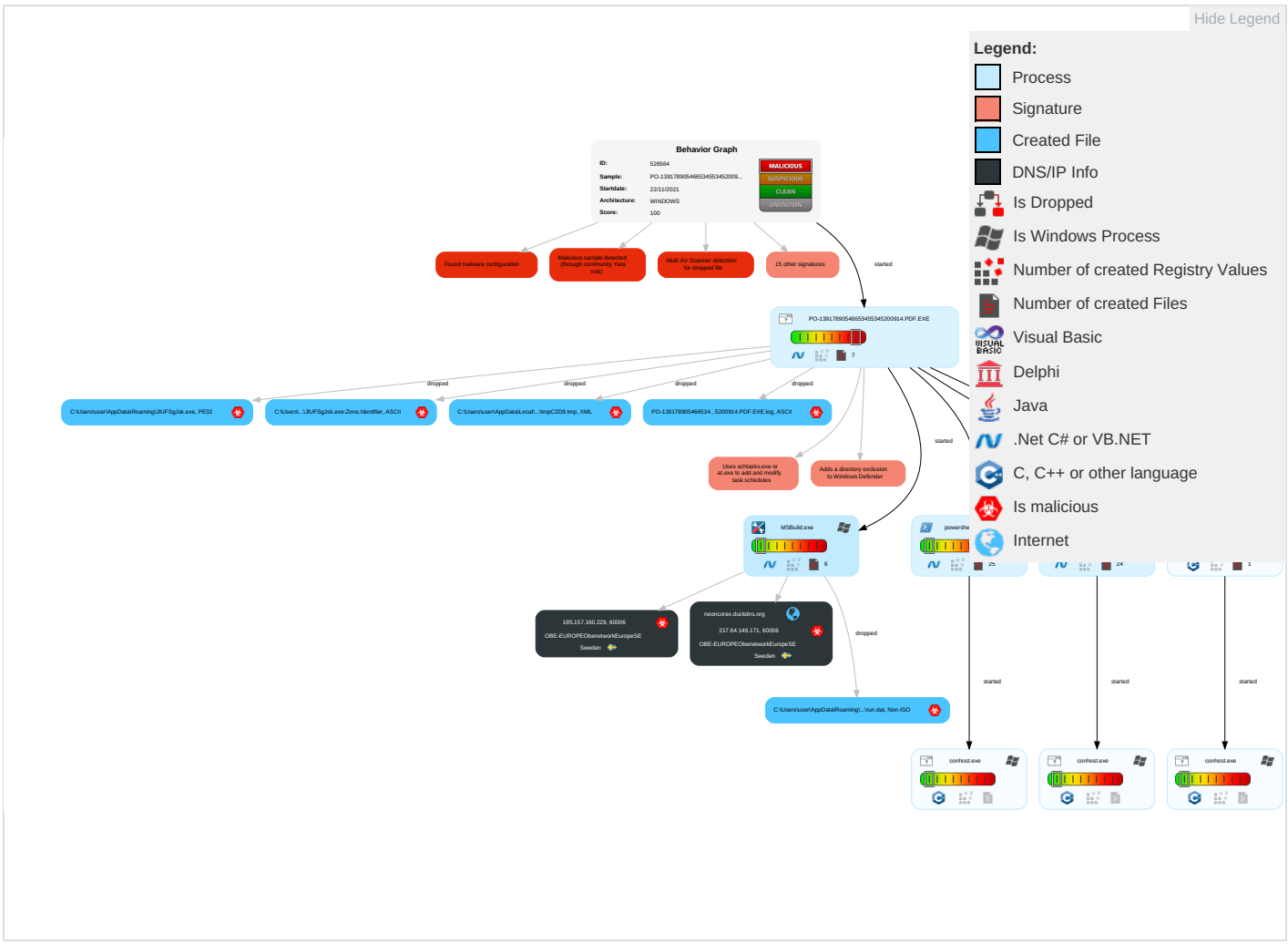
Detected Nanocore Rat

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	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po

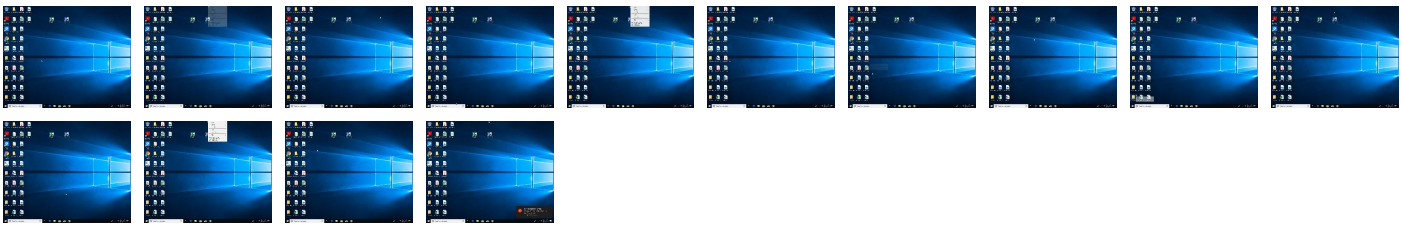
Behavior Graph



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
PO-139178905466534553452009 14.PDF.EXE	34%	Metadefender		Browse
PO-139178905466534553452009 14.PDF.EXE	51%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
PO-139178905466534553452009 14.PDF.EXE	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\JlUFSgJsk.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JlUFSgJsk.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Roaming\JlUFSgJsk.exe	51%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.MSBuild.exe.5750000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.MSBuild.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.MSBuild.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comeu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.elvoria.com/index.php	0%	Avira URL Cloud	safe	
http://www.fontbureau.comuef	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/soft	0%	URL Reputation	safe	
http://www.elvoria.com/index.php?error=noaccount	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comtU$	0%	Avira URL Cloud	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comalsC	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.com2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comC	0%	Avira URL Cloud	safe	
http://www.elvoria.com/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.elvoria.com/index.php?error=noaccountAhttp://www.elvoria.com/index.php	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://www.founder.com.cn/cncr	0%	Avira URL Cloud	safe	
neoncorex.duckdns.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comdito-	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comL.TTFH	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-u;	0%	Avira URL Cloud	safe	
http://www.elvoria.com/login.php	0%	Avira URL Cloud	safe	
http://www.sakkal.comp?	0%	Avira URL Cloud	safe	
185.157.160.229	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
neoncorex.duckdns.org	217.64.149.171	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
neoncorex.duckdns.org	true	• Avira URL Cloud: safe	unknown
185.157.160.229	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.64.149.171	neoncorex.duckdns.org	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
185.157.160.229	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526564
Start date:	22.11.2021
Start time:	18:53:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-139178905466534553452009 14.PDF.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:	27
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@12/12@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 0.8%) • Quality average: 36% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 90% • 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
18:54:39	API Interceptor	2x Sleep call for process: PO-139178905466534553452009 14.PDF.EXE modified
18:54:43	API Interceptor	75x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.64.149.171	PO-139166546588676543420067890 1012.exe	Get hash	malicious	Browse	
185.157.160.229	PO-139166546588676543420067890 1012.exe	Get hash	malicious	Browse	
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	
	DHL-300921676997653545562777564 8896.exe	Get hash	malicious	Browse	
	DHL-300921676997653545562777564 8893.exe	Get hash	malicious	Browse	
	dhl shipment_270921675766456346278586535672864757 37.pdf.exe	Get hash	malicious	Browse	
	NewProject-907255177625451771542544152425561 4.exe	Get hash	malicious	Browse	
	NewProject-907255177625451771542544152425561 4.exe	Get hash	malicious	Browse	
	kPFwk5vnfR.exe	Get hash	malicious	Browse	
	Attached pdf.exe	Get hash	malicious	Browse	
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
neoncorex.duckdns.org	PO-139166546588676543420067890 1012.exe	Get hash	malicious	Browse	• 217.64.149.171
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	• 185.157.16 0.229

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	Document.exe	Get hash	malicious	Browse	• 185.86.106.246
	luhgLCIALF.exe	Get hash	malicious	Browse	• 217.64.149.101
	PO-139166546588676543420067890 1012.exe	Get hash	malicious	Browse	• 185.157.16 0.229
	Solicitor Inquiry No. 0014921 - UK.xlsm	Get hash	malicious	Browse	• 217.64.149.101
	2j3X4garkJ.exe	Get hash	malicious	Browse	• 217.64.149.101
	PO-139166546588676543420067890 1000.exe	Get hash	malicious	Browse	• 185.157.16 0.229
	DOCUMENT.EXE	Get hash	malicious	Browse	• 185.86.106.246
	rHDCSXfW48.exe	Get hash	malicious	Browse	• 185.157.16 0.198
	W7rzSp83RC.exe	Get hash	malicious	Browse	• 185.157.16 0.198
	pT2Ty65w0q.exe	Get hash	malicious	Browse	• 185.157.16 0.198
	Wq95M8hSrX.exe	Get hash	malicious	Browse	• 185.157.16 0.198
	5tx1tCz0TC.exe	Get hash	malicious	Browse	• 185.157.16 0.198
	PO-139166546588676543420067890 06.exe	Get hash	malicious	Browse	• 185.157.16 0.229
	Document.exe	Get hash	malicious	Browse	• 217.64.149.78
	s7svHkrSTd.exe	Get hash	malicious	Browse	• 185.157.16 0.198

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Document.exe	Get hash	malicious	Browse	• 217.64.151.84
	Lj7T4BYEbQ.exe	Get hash	malicious	Browse	• 185.157.162.75
	13294_Video_Oynat#U0131c#U0131.apk	Get hash	malicious	Browse	• 178.132.78.156
	5alrKw7836.exe	Get hash	malicious	Browse	• 185.157.160.136
	Zakaz na pokupku 21-10-2021.doc	Get hash	malicious	Browse	• 185.157.160.136
OBE-EUROPEObenetworkEuropeSE	Document.exe	Get hash	malicious	Browse	• 185.86.106.246
	IuhgLClALF.exe	Get hash	malicious	Browse	• 217.64.149.101
	PO-139166546588676543420067890101 2.exe	Get hash	malicious	Browse	• 185.157.160.229
	Solicitor Inquiry No. 0014921 - UK.xlsm	Get hash	malicious	Browse	• 217.64.149.101
	2j3X4garkJ.exe	Get hash	malicious	Browse	• 217.64.149.101
	PO-139166546588676543420067890100 0.exe	Get hash	malicious	Browse	• 185.157.160.229
	DOCUMENT.EXE	Get hash	malicious	Browse	• 185.86.106.246
	rHDCSXfW48.exe	Get hash	malicious	Browse	• 185.157.160.198
	W7rzSp83RC.exe	Get hash	malicious	Browse	• 185.157.160.198
	pT2Ty65w0q.exe	Get hash	malicious	Browse	• 185.157.160.198
	Wq95M8hSrX.exe	Get hash	malicious	Browse	• 185.157.160.198
	5tx1tCz0TC.exe	Get hash	malicious	Browse	• 185.157.160.198
	PO-139166546588676543420 06.exe	Get hash	malicious	Browse	• 185.157.160.229
	Document.exe	Get hash	malicious	Browse	• 217.64.149.78
	s7svHkrSTd.exe	Get hash	malicious	Browse	• 185.157.160.198
	Document.exe	Get hash	malicious	Browse	• 217.64.151.84
	Lj7T4BYEbQ.exe	Get hash	malicious	Browse	• 185.157.162.75
	13294_Video_Oynat#U0131c#U0131.apk	Get hash	malicious	Browse	• 178.132.78.156
	5alrKw7836.exe	Get hash	malicious	Browse	• 185.157.160.136
	Zakaz na pokupku 21-10-2021.doc	Get hash	malicious	Browse	• 185.157.160.136

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO-139178905466534553452009 14.PDF.EXE.log	
Process:	C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO-139178905466534553452009 14.PDF.EXE.log	
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):	22376
Entropy (8bit):	5.60274040109138
Encrypted:	false
SSDEEP:	384:HtKDU82VN+ZyQbdplUqngS0ngjultIO7uB9gxISJ3x+T1MjPZlbAV7tTuZBDl+fC:l+U0pG8gTgCltR7+c8C7fwpKV1C
MD5:	C962158D9DE14FF5B13EC094263838DF
SHA1:	D5FE4F32494480B5852915FC4B485476CADB7A67
SHA-256:	89AC2D261F9E059B55529F88093B5096223AF7B0CA0FE419A839E5AA3FE1DB91
SHA-512:	05DA6A96514698DD1639CDFC7546F044631A86B2037A9E5DE3A87956041860142B776B7BAB5E5578762206D6B32B3914E32D6736BC5FF0227660290B37026AE3
Malicious:	false
Preview:	@...e.....e...H.@.=.....F.....@.....H.....<@.^.L."My...:P..... .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.L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j0vmi1oo.4vc.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mqqok3ey.rsj.ps1	
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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mzqv2te3.s4z.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mzqv2te3.s4z.psm1	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uqylmfg2.jq4.ps1	
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
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpC2D8.tmp	
Process:	C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1596
Entropy (8bit):	5.152229811063346
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtdxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTjv
MD5:	EF2D169434860F3DFBF1B43C9A84D0A1
SHA1:	47E142BCC66D171BE211153297C328E300B58073
SHA-256:	14FA2717EB4C611F088C596B047C7696EC0CD6B9880906AFBC764F4DADAE8900
SHA-512:	2E5DC44FB6038FEF50D6BDB12BC98C72B6F4ABBFF3AC5A90A7B17882DD5BA51E19E66F33EA99343328A685F395275BE45B58CF41C22AB613EAD87C459553E7CE
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</StartWhenAvailable>. <

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:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:eKEQ:e2
MD5:	F4B927879C434BD317A04D5A0B760AE1
SHA1:	A7BB61B40C2F8729047A12C8CF69ED82ABA436D0
SHA-256:	CA49E6943AFE422EDCF7EF2A338B17E78BA9ED262449E30E48FD03D23B005BC3
SHA-512:	8AA4D9CBF74449C50E83E29E5297806FA5A56E3F3A18F4F396231C696885E7B0D14ED642518BDE5117F34098E2ED0F7D4C6F36CE88349B2967CE324982B7106C
Malicious:	**true**
Preview:	...,..H

C:\Users\user\AppData\Roaming\JlUFSgJsk.exe	
Process:	C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	945152
Entropy (8bit):	6.97885031884941
Encrypted:	false
SSDEEP:	12288:2WdV9V9Ve0j/0cu2ooTmBnRmTaayF+tlX7cPQpSH2AYLbT5EeVD:2uV9V9VxX2nwjpSdYLD
MD5:	84449B1242CB54AFC4BB3E9B628FDFAC
SHA1:	5E652729685A2717FF71BFFD51B6FD3F5614196D
SHA-256:	2B8ACFA28705C8321A35E0A22F554E56B5007D2D4E383061EC3DA0FB9658AECA
SHA-512:	DC98334BA7F0DE45A75300D425CB0A2164321228198115A808E90C436575EB7F5B89545776F9A749DD21BEBF7C8FDD35A77D0637A8FA08E3AD87B5C209D36AE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 51%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O..a.....0..@...*.....N_... ...`....@.. .....@.....^..W....`...&..... ....H.....text...T?... ...@..... ..`.rsrc....&...`...(...B..... ..@..@.reloc.....j.....@..B.....0_.....H.....T.....Q.....0.....*....0.....(.....*.0..{.....}.....}.....}.....(.... 1p.o ...ga%..^E..... .....".=.....+;.. c.yZ .u..a+... s!/.Z S.2)a+..(.....(^.... ..T.Z C(S.a+..*..0..... f!.. cz..a%..^E....6...W.....+U.s ...}..... 8..'Z ...a+..{..... MX.TZ ..3.a+....{....s....}..... .CC.Z ..a+.*....0.....{....o!...~"...(#.....,W 4..\ b"qxa%..^E.....P.....3...+N.{.....{....o!..

C:\Users\user\AppData\Roaming\JlUFSgJsk.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211122\PowerShell_transcript.618321.fCS6NoyN.20211122185441.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):	5849
Entropy (8bit):	5.442426189476261
Encrypted:	false
SSDEEP:	96:BZuhCMNuqDo1ZJZvhCMNuqDo1ZAYSwjZ3hCMNuqDo1ZHtggHZA:LCm+
MD5:	797AD35BEDA046E298BF19CB9DC2112A
SHA1:	A653451F2F1C1166377D3956B6188BAEF7BDB3E8
SHA-256:	75700861B2E80B6431DAB49A315188757C619A4478FBA1D215D59268642D4E34
SHA-512:	9D156C3404540BF47AD64CEEA8ACCFA7B1173277E9B63A687AFF8F664A51F58FEAFAE3ED6250A4A75A9412691F782D49143FDE3A102E32CD554A0A57976853A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122185443..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE..Process ID: 2892..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatible Versions: 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: 20211122185443..**********..PS>Add-MpPreference -Exclusion Path C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE..**********..Windows PowerShell transcript start..Start time: 20211122185811..Usern ame: computer\user..Ru

C:\Users\user\Documents\20211122\PowerShell_transcript.618321.gbK9sM4K.20211122185443.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):	5785
Entropy (8bit):	5.411461908952191
Encrypted:	false
SSDEEP:	96:BZdhCMNqUqDo1ZiZahCMNqUqDo1ZBeM2jZHhCMNqUqDo1ZxXmmDZk:Wbi1

C:\Users\user\Documents\20211122\PowerShell_transcript.618321.gbK9sM4K.20211122185443.txt	
MD5:	73E27B8634CB3CCA7352310AF76381D4
SHA1:	BE67ADE2C393291F542635BEB36FD092D50B679B
SHA-256:	B3FFA5C4E7FBAA6FD79AF16F6A0303749AA1759BCEDB4B91816937C4FC2336FA
SHA-512:	D5762F90974482FF138AFEBB6A6FA54A5A9B3E1BCFFDF2A75FAAF06B2ED3F3074D82A35503F38A1D36B7EBF302FE45BE8645961975B45A8E5909D0999B032A58
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122185444..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (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\JlUFSgJsk.exe..Process ID: 5320..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: 20211122185444..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\JlUFSgJsk.exe..**********..Windows PowerShell transcript start..Start time: 20211122185757..Username: computer\user..RunAs User: computer\user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.97885031884941
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:	PO-139178905466534553452009l4.PDF.EXE
File size:	945152
MD5:	84449b1242cb54afc4bb3e9b628fdfac
SHA1:	5e652729685a2717ff71bffd51b6fd3f5614196d
SHA256:	2b8acfa28705c8321a35e0a22f554e56b5007d2d4e38306 1ec3da0fb9658aeca
SHA512:	dc98334ba7f0de45a75300d425cb0a2164321228198115 a808e90c436575eb7f5b89545776f9a749dd21bebf7c8fd d35a77d0637a8fa08e3ad87b5c209d36aee
SSDEEP:	12288:2WdV9V9Ve0j/0cu2ooTmBnRmTaayF+tlX7cPQ pSH2AYLbT5EeVD:2uV9V9VxX2nwjpSdYLD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O..a.....0..@...*.....N_... ...`....@.. ....@.....

File Icon

Icon Hash:	27e78386858d8993

Static PE Info

General

Entrypoint:	0x4a5f4e
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:	0x6197824F [Fri Nov 19 10:54:07 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

General

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	0xa3f54	0xa4000	False	0.719803972942	data	7.36961053768	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x426e0	0x42800	False	0.24775684328	data	4.85371440871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-18:55:47.004978	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49572	8.8.8.8	192.168.2.3
11/22/21-18:56:05.464834	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60823	8.8.8.8	192.168.2.3
11/22/21-18:56:22.224988	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55102	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 18:55:46.886960030 CET	192.168.2.3	8.8.8.8	0xc8f	Standard query (0)	neoncorex.duckdns.org	A (IP address)	IN (0x0001)
Nov 22, 2021 18:56:05.346734047 CET	192.168.2.3	8.8.8.8	0xd9d4	Standard query (0)	neoncorex.duckdns.org	A (IP address)	IN (0x0001)
Nov 22, 2021 18:56:22.109146118 CET	192.168.2.3	8.8.8.8	0x79b6	Standard query (0)	neoncorex.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 18:55:47.004977942 CET	8.8.8.8	192.168.2.3	0xc8f	No error (0)	neoncorex.duckdns.org		217.64.149.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 18:56:05.464833975 CET	8.8.8.8	192.168.2.3	0xd9d4	No error (0)	neoncorex.duckdns.org		217.64.149.171	A (IP address)	IN (0x0001)
Nov 22, 2021 18:56:22.224987984 CET	8.8.8.8	192.168.2.3	0x79b6	No error (0)	neoncorex.duckdns.org		217.64.149.171	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO-139178905466534553452009 14.PDF.EXE PID: 5672 Parent PID: 6012

General

Start time:	18:54:32
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO-139178905466534553452009 14.PDF.EXE"
Imagebase:	0xde0000
File size:	945152 bytes
MD5 hash:	84449B1242CB54AFC4BB3E9B628FDFAC
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: 00000001.00000002.324098366.00000000031B3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.324315538.000000000330F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.324825030.00000000041BC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.324825030.00000000041BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.324825030.00000000041BC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2892 Parent PID: 5672

General

Start time:	18:54:40
Start date:	22/11/2021
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\Desktop\PO-139178905466534553452009 14.PDF.EXE
Imagebase:	0xf30000
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: 5016 Parent PID: 2892

General

Start time:	18:54:41
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: powershell.exe PID: 5320 Parent PID: 5672

General

Start time:	18:54:42
Start date:	22/11/2021
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\JlUFSgJsk.exe

Imagebase:	0xf30000
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: 5100 Parent PID: 5320

General

Start time:	18:54:42
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 1760 Parent PID: 5672

General

Start time:	18:54:42
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JlUFSgJsk" /XML "C:\Users\user\AppData\Local\Temp\tmpC2D8.tmp
Imagebase:	0xff0000
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: 1312 Parent PID: 1760

General

Start time:	18:54:43
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 6532 Parent PID: 5672

General

Start time:	18:54:45
Start date:	22/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x8f0000
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: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.321914533.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.321914533.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.321914533.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.557435379.0000000003CC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.557435379.0000000003CC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.558396997.0000000005750000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.558396997.0000000005750000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.558396997.0000000005750000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.321330951.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.321330951.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.321330951.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.319503171.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.319503171.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.319503171.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.558298793.00000000055F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.558298793.00000000055F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.320448358.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.320448358.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.320448358.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.555044051.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.555044051.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.555044051.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis