ID: 527111
Sample Name: Orden de Compra -SA765443,pdf.exe
Cookbook: default.jbs
Time: 11:58:19
Date: 23/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

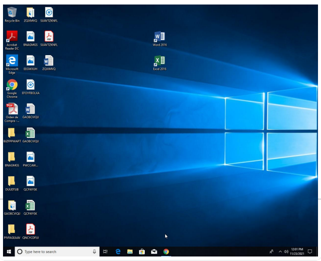
Windows Analysis Report Orden de Compra -SA765443,…

Overview

General Information

Sample Name:	Orden de Compra -SA765443,pdf.exe
Analysis ID:	527111
MD5:	f7f223c7625c5c9..
SHA1:	2105dc6b41d1ec..
SHA256:	7a356a718b0ca6..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

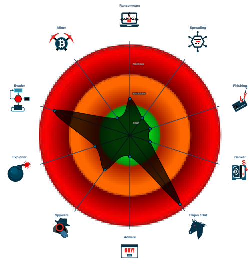
Nanocore

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

Signatures

- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- Orden de Compra -SA765443,pdf.exe (PID: 6196 cmdline: "C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe" MD5: F7F223C7625C5C9DF43AF835298C1183)
  - Orden de Compra -SA765443,pdf.exe (PID: 6548 cmdline: C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe MD5: F7F223C7625C5C9DF43AF835298C1183)
    - schtasks.exe (PID: 6712 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp62E7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Orden de Compra -SA765443,pdf.exe (PID: 6864 cmdline: "C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe" 0 MD5: F7F223C7625C5C9DF43AF835298C1183)
  - Orden de Compra -SA765443,pdf.exe (PID: 4220 cmdline: C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe MD5: F7F223C7625C5C9DF43AF835298C1183)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c78d90a0-5de6-4b77-9d98-da24b367",
  "Group": "CHIBOY",
  "Domain1": "wealthgod1234.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 4693,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 4995,
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.310703445.0000000004239000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000002.310703445.0000000004239000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435d5:$a: NanoCore • 0x4362e:$a: NanoCore • 0x4366b:$a: NanoCore • 0x436e4:$a: NanoCore • 0x56d8f:$a: NanoCore • 0x56da4:$a: NanoCore • 0x56dd9:$a: NanoCore • 0x6fd7b:$a: NanoCore • 0x6fd90:$a: NanoCore • 0x6fdc5:$a: NanoCore • 0x43637:$b: ClientPlugin • 0x43674:$b: ClientPlugin • 0x43f72:$b: ClientPlugin • 0x43f7f:$b: ClientPlugin • 0x56b4b:$b: ClientPlugin • 0x56b66:$b: ClientPlugin • 0x56b96:$b: ClientPlugin • 0x56dad:$b: ClientPlugin • 0x56de2:$b: ClientPlugin • 0x6fb37:$b: ClientPlugin • 0x6fb52:$b: ClientPlugin
00000000.00000002.266827018.0000000002CA1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000000.262435507.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000000.262435507.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 60 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Orden de Compra -SA765443,pdf.exe.3d02698.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Orden de Compra -SA765443,pdf.exe.3d02698.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.Orden de Compra -SA765443,pdf.exe.3d02698.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Orden de Compra -SA765443,pdf.exe.3d02698.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
14.0.Orden de Compra -SA765443,pdf.exe.400000.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 116 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

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
- Yara detected Nanocore RAT

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)

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:

- Icon mismatch, binary includes an icon from a different legit application in order to fool users
- Hides that the sample has been downloaded from the Internet (zone.identifier)

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:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

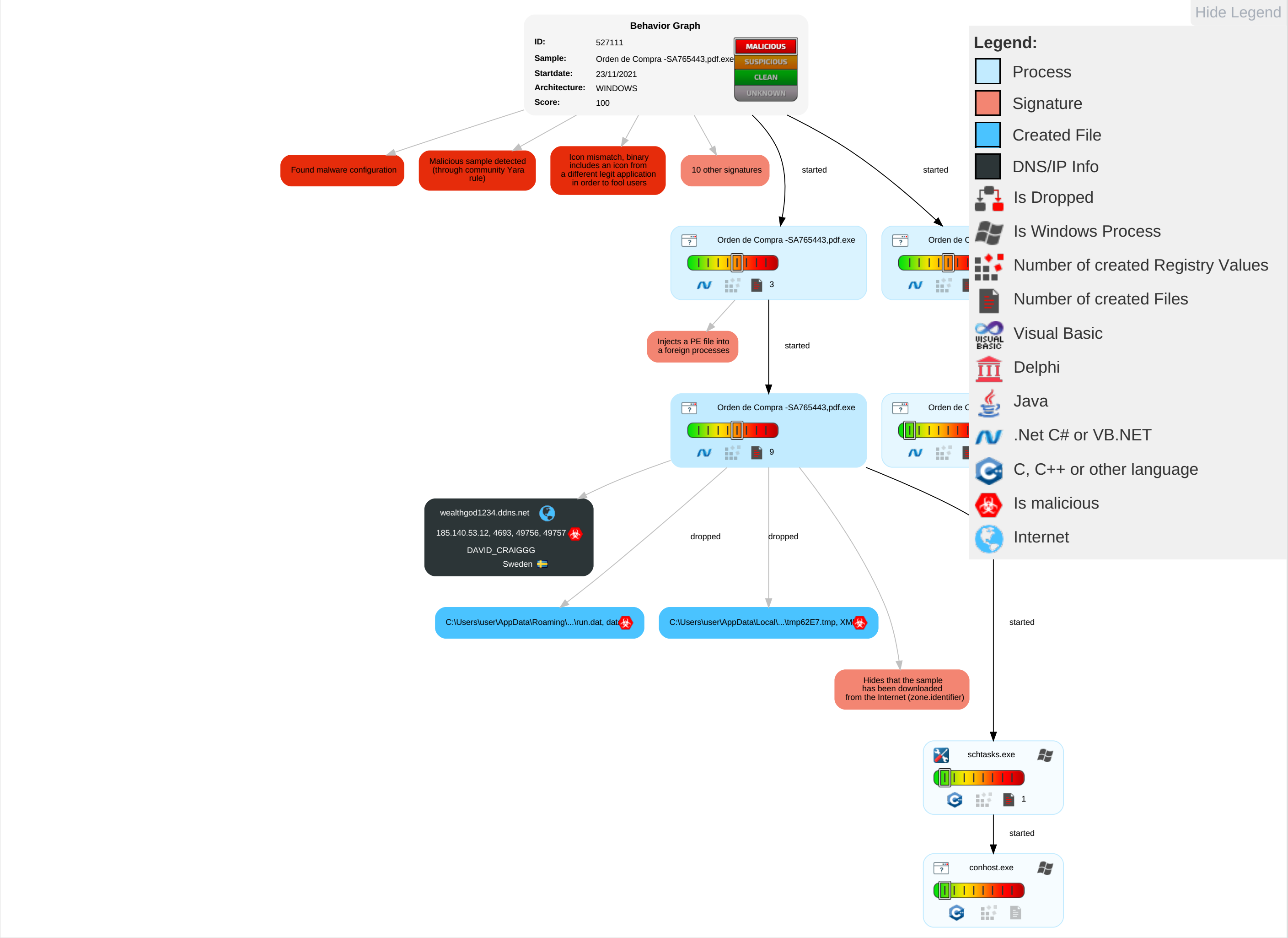
Remote Access Functionality:

- 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	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 2 1	Security Software Discovery 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/
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	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downl Insecu Protoc

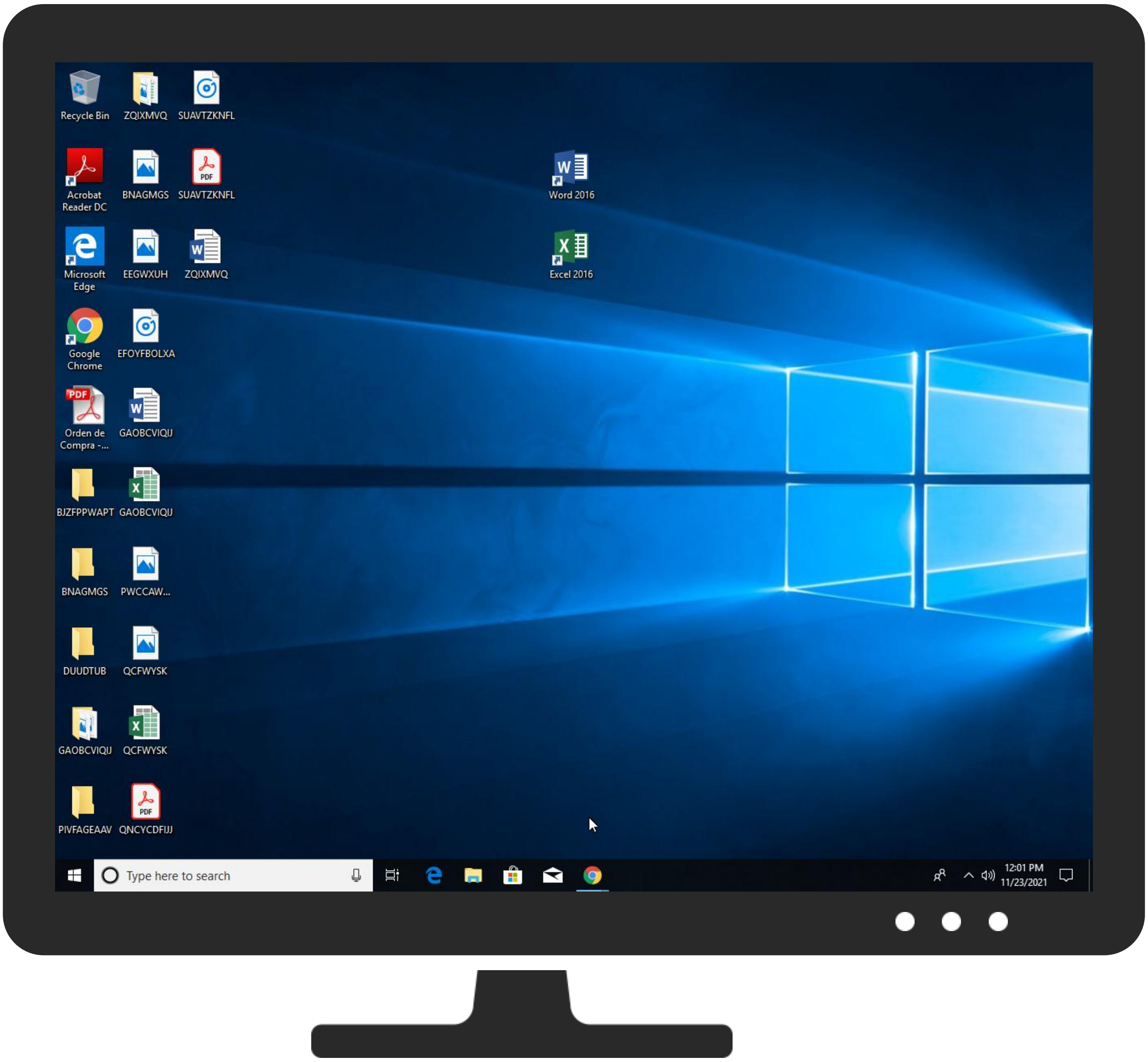
Behavior Graph


Hide Legend
Behavior Graph
ID: 527111
Sample: Orden de Compra -SA765443,pdf.exe
Startdate: 23/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Icon mismatch, binary includes an icon from a different legit application in order to fool users
10 other signatures
started
started
Orden de Compra -SA765443,pdf.exe
3
Orden de C
Injects a PE file into a foreign processes
started
Orden de Compra -SA765443,pdf.exe
9
Orden de C
wealthgod1234.ddns.net
185.140.53.12, 4693, 49756, 49757
DAVID_CRAIGGG
Sweden
dropped
dropped
C:\Users\user\AppData\Roaming\...\run.dat, data
C:\Users\user\AppData\Local\...\tmp62E7.tmp, XML
Hides that the sample has been downloaded from the Internet (zone.identifier)
started
schtasks.exe
1
started
conhost.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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
5.2.Orden de Compra -SA765443,pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.Orden de Compra -SA765443,pdf.exe.66b0000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.0.Orden de Compra -SA765443,pdf.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Orden de Compra -SA765443,pdf.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Orden de Compra -SA765443,pdf.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.Orden de Compra -SA765443,pdf.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Orden de Compra -SA765443,pdf.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.Orden de Compra -SA765443,pdf.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.Orden de Compra -SA765443,pdf.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Orden de Compra -SA765443,pdf.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.Orden de Compra -SA765443,pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.Orden de Compra -SA765443,pdf.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Orden de Compra -SA765443,pdf.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
wealthgod1234.ddns.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
wealthgod1234.ddns.net	2%	Virustotal		Browse
wealthgod1234.ddns.net	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	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.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthgod1234.ddns.net	185.140.53.12	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wealthgod1234.ddns.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.12	wealthgod1234.ddns.net	Sweden	🇸🇪	209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	527111
Start date:	23.11.2021
Start time:	11:58:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orden de Compra -SA765443,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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/5@16/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.4%) • Quality average: 26.6% • Quality standard deviation: 36%
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
11:59:21	API Interceptor	921x Sleep call for process: Orden de Compra -SA765443,pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.12	Hemotronik Nov Acil PO_76565,pdf.exe	Get hash	malicious	Browse	
	SOMECO Nov Acil PO_76565,pdf.exe	Get hash	malicious	Browse	
	Sifari#U015fin t#U0259sdiq edilm#U0259si _ T#U0259 cili,pdf.exe	Get hash	malicious	Browse	
	AWB # 2617429350,pdf.exe	Get hash	malicious	Browse	
	AWB # 2617429350,pdf.exe	Get hash	malicious	Browse	
	C.GNew pedido WJO-001,pdf.exe	Get hash	malicious	Browse	
	DHL_119040 re#U00e7u,pdf (2).exe	Get hash	malicious	Browse	
	Confirmaci#U00f3n de pedido nuevo-5309,pdf.exe	Get hash	malicious	Browse	
	Urgente RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	
	Urgent RFQ_AP65425652_03242,pdf.exe	Get hash	malicious	Browse	
	vmw7WdkJ6k.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CONTRACT PMA1911003.exe	Get hash	malicious	Browse	
	003663-37399.exe	Get hash	malicious	Browse	
	BingUpdate.exe	Get hash	malicious	Browse	
	Documents RF V23665.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	purchase order 0112.exe	Get hash	malicious	Browse	• 185.140.53.137
	9mMANDmw9O.exe	Get hash	malicious	Browse	• 91.193.75.190
	TR0398734893 50601251.exe	Get hash	malicious	Browse	• 185.140.53.131
	swift.xls	Get hash	malicious	Browse	• 91.193.75.212
	SOA_0009877890.exe	Get hash	malicious	Browse	• 185.244.30.58
	8UYr1od7iW.exe	Get hash	malicious	Browse	• 91.193.75.148
	928272_Payment_Receipt.vbs	Get hash	malicious	Browse	• 185.140.53.3
	N2K18_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	U2M19O_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	J3m1a_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	18-11-21 Statement.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	bWKXCwatmt.exe	Get hash	malicious	Browse	• 91.193.75.148
	17-11-21 STATEMENT.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	Copy of Complaint report-1st Nov21 to 16th Nov21.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	UTYHFG03983765367839837653.exe	Get hash	malicious	Browse	• 185.140.53.131
	IkGcQX45T8.exe	Get hash	malicious	Browse	• 91.193.75.148
	vcjjMWSZx8.exe	Get hash	malicious	Browse	• 185.140.53.138
	000876543234567.exe	Get hash	malicious	Browse	• 185.244.30.58
	Dhl_Shipment_one.exe	Get hash	malicious	Browse	• 185.140.53.137
	PO.E210115.exe	Get hash	malicious	Browse	• 185.244.30.252

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Orden de Compra -SA765443,pdf.exe.log	
Process:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Orden de Compra -SA765443,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\Temp\tmp62E7.tmp	
Process:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1323
Entropy (8bit):	5.12284374389714
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0kxtn:cbk4oL600QydbQxIYODOLedq3Jj
MD5:	38A67D49BD1B250B49E9E6A7ECD6CD14
SHA1:	4FDD0D9B3F3E4E5B48CA231343324E30951BE2E3
SHA-256:	6DD0B3C0DFA7950B1DEDA930882F3E84912932021A76F853561BA640816D4251
SHA-512:	86DB3AF07E0180504DCBFCE1FC1BC7F6A00F12BD8AF76774382E3B4CEF4BD5ED9FBDEE8089F772AA075B973257C922C4E89C279B4E09362173794617B7BF60A C
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	128
Entropy (8bit):	6.527114648336088
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRH5/ljRAaTlKYrI1Sj9txROIsxcMek2:X4LDAn1rplKTYBROIsxek2
MD5:	0A9C5EAE8756D6FC90F59D8D71A79E1E
SHA1:	0F7D6AAED17CD18DC614535ED26335C147E29ED7
SHA-256:	B1921EA14C66927397BAF3FA456C22B93C30C3DE23546087C0B18551CE5001C5
SHA-512:	78C2F399AC49C78D89915DFF99AC955B5E0AB07BAAD61B07B0CE073C88C1D3A9F1D302C2413691B349DD34441B0FF909C08A4F71E2F1B73F46C1FF308BC7CF A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P.OT....g.t......'7......)..8zII..K/....n3...3.5.......&.7].)..wL...:}g...@...mV.....JUP...w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:0keIt:0A
MD5:	94B41CFEE4E2B49BD4C1E82A95852AF4
SHA1:	4BB08756493EB9A0E663E0688E451841BC9BE9CD
SHA-256:	42CE8F756A9AF3726B6EFDA3823B0DBB539AB1EDF322B08B807E4ADD86A819E7
SHA-512:	96A9FC234C38C2D983CE8EED8823EF3F9E2E907B6EE967DEF3981F7ED6E351654F58B98B5877A3620D2FC84C0171EB9DA92BC3B0EA8B030ABCD78B8CE90423 BF
Malicious:	**true**
Reputation:	low
Preview:	.>.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.608288146260291
Encrypted:	false
SSDEEP:	3:oN0naRRqXIgq9EDDJ:oNcSRqXIFED9
MD5:	FC28A690D1E29EEEC388DFB51CCB3449
SHA1:	D20184CB0468F8BA3D1481A9BD72CB8956FB10AA
SHA-256:	5DC03F18C097ACE50982402ED7A9829F8ECDAEAFC6E048147E5AA871DEEF845F
SHA-512:	B1B8A12EC1EAB4634BE96CD46D1B24AA2B1797E531EAB965DE4BE752CB0B1CED61713FDF4B635F76B10F92A3E9AE62C6D7087F9BD4E5758BF6062E31AB165C07
Malicious:	false
Preview:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.69147440283363
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:	Orden de Compra -SA765443,pdf.exe
File size:	577536
MD5:	f7f223c7625c5c9df43af835298c1183
SHA1:	2105dc6b41d1ec220e89fb018fb1fd95b9a22d5a
SHA256:	7a356a718b0ca6272486633efb6a34c6301007f50766d8cfab60a996f2729935
SHA512:	0238b920a0f2afc3df08c5634573037eaf649464f0324afc3a1bc1ca1aafe858bb31e75feb1c487cdbf6a8496a5128c21fda112fe439c45299f10d853a0ed290
SSDEEP:	12288:sglS4oq0RueU5AzUJCjKs7pw2i/FB8r7S5Ud3EWtD00UxZ:NlSoEfUAWE7UFS3cUWWC0Ux
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......a..............0......D........... ....@.. ....@...........@................................

File Icon

Icon Hash:	c49a0894909c6494

Static PE Info

General

Entrypoint:	0x48a81e
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:	0x619CB29F [Tue Nov 23 09:21:35 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x88824	0x88a00	False	0.853445934355	data	7.72977166234	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x4200	0x4200	False	0.455669981061	data	5.72908968706	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/23/21-11:59:33.326172	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54640	8.8.8.8	192.168.2.7
11/23/21-11:59:39.867599	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58739	8.8.8.8	192.168.2.7
11/23/21-11:59:52.949500	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59762	8.8.8.8	192.168.2.7
11/23/21-12:00:21.346042	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50781	8.8.8.8	192.168.2.7
11/23/21-12:00:28.959265	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50452	8.8.8.8	192.168.2.7
11/23/21-12:00:49.940231	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49247	8.8.8.8	192.168.2.7
11/23/21-12:00:56.951611	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56064	8.8.8.8	192.168.2.7
11/23/21-12:01:11.033668	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61457	8.8.8.8	192.168.2.7
11/23/21-12:01:18.086716	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58367	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2021 11:59:33.304900885 CET	192.168.2.7	8.8.8.8	0xfe0d	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:39.846254110 CET	192.168.2.7	8.8.8.8	0x6ab8	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:46.156789064 CET	192.168.2.7	8.8.8.8	0x5df9	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:52.927398920 CET	192.168.2.7	8.8.8.8	0x1e6a	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:59.120119095 CET	192.168.2.7	8.8.8.8	0x4104	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:06.133011103 CET	192.168.2.7	8.8.8.8	0x8c5d	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:14.324692011 CET	192.168.2.7	8.8.8.8	0x4d13	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:21.321403027 CET	192.168.2.7	8.8.8.8	0xfab1	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:28.937688112 CET	192.168.2.7	8.8.8.8	0xc73e	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:35.907048941 CET	192.168.2.7	8.8.8.8	0x2e41	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:43.069562912 CET	192.168.2.7	8.8.8.8	0x6ff	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:49.920238972 CET	192.168.2.7	8.8.8.8	0x6285	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:56.928706884 CET	192.168.2.7	8.8.8.8	0xd645	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:01:03.983671904 CET	192.168.2.7	8.8.8.8	0xf269	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:01:11.011229992 CET	192.168.2.7	8.8.8.8	0xd872	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 12:01:18.065009117 CET	192.168.2.7	8.8.8.8	0x2040	Standard query (0)	wealthgod1234.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 11:59:33.326172113 CET	8.8.8.8	192.168.2.7	0xfe0d	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:39.867599010 CET	8.8.8.8	192.168.2.7	0x6ab8	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:46.177053928 CET	8.8.8.8	192.168.2.7	0x5df9	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:52.949500084 CET	8.8.8.8	192.168.2.7	0x1e6a	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 11:59:59.140615940 CET	8.8.8.8	192.168.2.7	0x4104	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:06.153048038 CET	8.8.8.8	192.168.2.7	0x8c5d	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:14.345205069 CET	8.8.8.8	192.168.2.7	0x4d13	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:21.346041918 CET	8.8.8.8	192.168.2.7	0xfab1	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:28.959264994 CET	8.8.8.8	192.168.2.7	0xc73e	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:35.926978111 CET	8.8.8.8	192.168.2.7	0x2e41	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:43.087691069 CET	8.8.8.8	192.168.2.7	0x6ff	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:49.940231085 CET	8.8.8.8	192.168.2.7	0x6285	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:00:56.951611042 CET	8.8.8.8	192.168.2.7	0xd645	No error (0)	wealthgod1234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 12:01:04.004245996 CET	8.8.8.8	192.168.2.7	0xf269	No error (0)	wealthgod1 234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:01:11.033668041 CET	8.8.8.8	192.168.2.7	0xd872	No error (0)	wealthgod1 234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)
Nov 23, 2021 12:01:18.086715937 CET	8.8.8.8	192.168.2.7	0x2040	No error (0)	wealthgod1 234.ddns.net		185.140.53.12	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Orden de Compra -SA765443,pdf.exe PID: 6196 Parent PID: 6008

General

Start time:	11:59:13
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe"
Imagebase:	0x860000
File size:	577536 bytes
MD5 hash:	F7F223C7625C5C9DF43AF835298C1183
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: 00000000.00000002.266827018.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.266922252.0000000002CDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.268195690.0000000003CA9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.268195690.0000000003CA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.268195690.0000000003CA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Orden de Compra -SA765443,pdf.exe PID: 6548 Parent PID: 6196

General

Start time:	11:59:22
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
Imagebase:	0xcf0000
File size:	577536 bytes
MD5 hash:	F7F223C7625C5C9DF43AF835298C1183
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: 00000005.00000000.262435507.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.262435507.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.262435507.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.516892703.00000000066B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.516892703.00000000066B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.516892703.00000000066B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.261948516.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.261948516.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.261948516.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.512725162.0000000003001000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.263642925.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.263642925.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.263642925.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.516734883.0000000005AD0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.516734883.0000000005AD0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.262924739.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.262924739.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.262924739.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.514335905.000000000404D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.507112354.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.507112354.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.507112354.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6712 Parent PID: 6548

General

Start time:	11:59:27
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp62E7.tmp
Imagebase:	0x170000
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: 6728 Parent PID: 6712

General

Start time:	11:59:29
Start date:	23/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Orden de Compra -SA765443,pdf.exe PID: 6864 Parent PID: 1104

General

Start time:	11:59:31
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe" 0
Imagebase:	0xdb0000
File size:	577536 bytes
MD5 hash:	F7F223C7625C5C9DF43AF835298C1183
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: 00000009.00000002.294956289.0000000003201000.00000004.00000001.sdmp, Author: Joe Security - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.296236042.0000000004209000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.296236042.0000000004209000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000009.00000002.296236042.0000000004209000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.295061035.000000000323E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: Orden de Compra -SA765443,pdf.exe PID: 4220 Parent PID: 6864

General

Start time:	11:59:35
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Orden de Compra -SA765443,pdf.exe
Imagebase:	0xea0000
File size:	577536 bytes
MD5 hash:	F7F223C7625C5C9DF43AF835298C1183
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: 0000000E.00000002.310703445.0000000004239000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.310703445.0000000004239000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.289660204.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.289660204.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.289660204.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.309326840.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.309326840.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.309326840.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.290829502.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.290829502.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.290829502.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.310601454.0000000003231000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.310601454.0000000003231000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.292078484.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.292078484.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.292078484.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.291488537.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.291488537.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.291488537.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis