ID: 509323
Sample Name: Payment Notification.pdf.scr
Cookbook: default.jbs
Time: 12:06:34
Date: 26/10/2021
Version: 33.0.0 White Diamond

Table of Contents

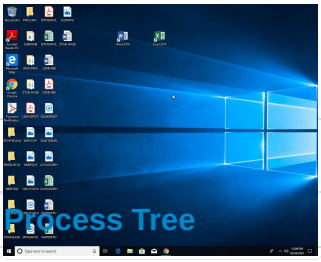
Windows Analysis Report Payment Notification.pdf.scr

Overview

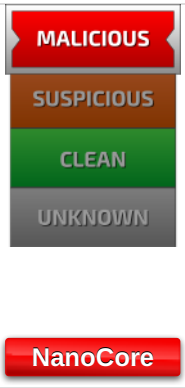
General Information

Sample Name:	Payment Notification.pdf.scr (renamed file extension from scr to exe)
Analysis ID:	509323
MD5:	06e79cb697e436..
SHA1:	025758750ef682c.
SHA256:	07749072a852c7..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

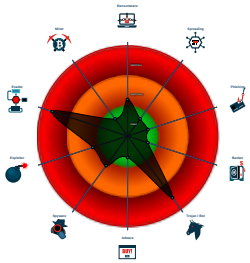


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…

Classification



- **System is w10x64**
- Payment Notification.pdf.exe (PID: 6132 cmdline: 'C:\Users\user\Desktop\Payment Notification.pdf.exe' MD5: 06E79CB697E436C1E66C49D3C39DBD82)
  - schtasks.exe (PID: 3740 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XDyfQvRGNV' /XML 'C:\Users\user\AppData\Local\Temp\tmpB5A6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5412 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ed2d5ce0-ca4d-4264-be01-91a018d5",
  "Domain1": "harold.accesscam.org",
  "Domain2": "harold.2waky.com",
  "Port": 6051,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "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
00000000.00000002.681190398.000000000300 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.681509296.000000000400 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x29efcd:$x1: NanoCore.ClientPluginHost • 0x2d17ed:$x1: NanoCore.ClientPluginHost • 0x29f00a:$x2: IClientNetworkHost • 0x2d182a:$x2: IClientNetworkHost • 0x2a2b3d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x2d535d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.681509296.000000000400 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.681509296.000000000400 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x29ed35:$a: NanoCore • 0x29ed45:$a: NanoCore • 0x29ef79:$a: NanoCore • 0x29ef8d:$a: NanoCore • 0x29efcd:$a: NanoCore • 0x2d1555:$a: NanoCore • 0x2d1565:$a: NanoCore • 0x2d1799:$a: NanoCore • 0x2d17ad:$a: NanoCore • 0x2d17ed:$a: NanoCore • 0x29ed94:$b: ClientPlugin • 0x29ef96:$b: ClientPlugin • 0x29efd6:$b: ClientPlugin • 0x2d15b4:$b: ClientPlugin • 0x2d17b6:$b: ClientPlugin • 0x2d17f6:$b: ClientPlugin • 0x16783e:$c: ProjectData • 0x1bb65e:$c: ProjectData • 0x29eebb:$c: ProjectData • 0x2d16db:$c: ProjectData • 0x29f8c2:$d: DESCrypto
Process Memory Space: Payment Notification.pdf.exe PID: 6132	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.Payment Notification.pdf.exe.428fe40.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x429ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x429ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Payment Notification.pdf.exe.428fe40.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x42725:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x429ad:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x43fe6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x43fda:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x44e8b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x4ac42:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost • 0x429d7:$s5: IClientLoggingHost
0.2.Payment Notification.pdf.exe.428fe40.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Payment Notification.pdf.exe.428fe40.2.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x42715:$a: NanoCore • 0x42725:$a: NanoCore • 0x42959:$a: NanoCore • 0x4296d:$a: NanoCore • 0x429ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x42774:$b: ClientPlugin • 0x42976:$b: ClientPlugin • 0x429b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x4289b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x432a2:$d: DESCrypto • 0x1844e:$e: KeepAlive
0.2.Payment Notification.pdf.exe.428fe40.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 10 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

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

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
Executable has a suspicious name (potential lure to open the executable)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)
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:

Writes to foreign memory regions
Allocates memory in foreign processes
Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

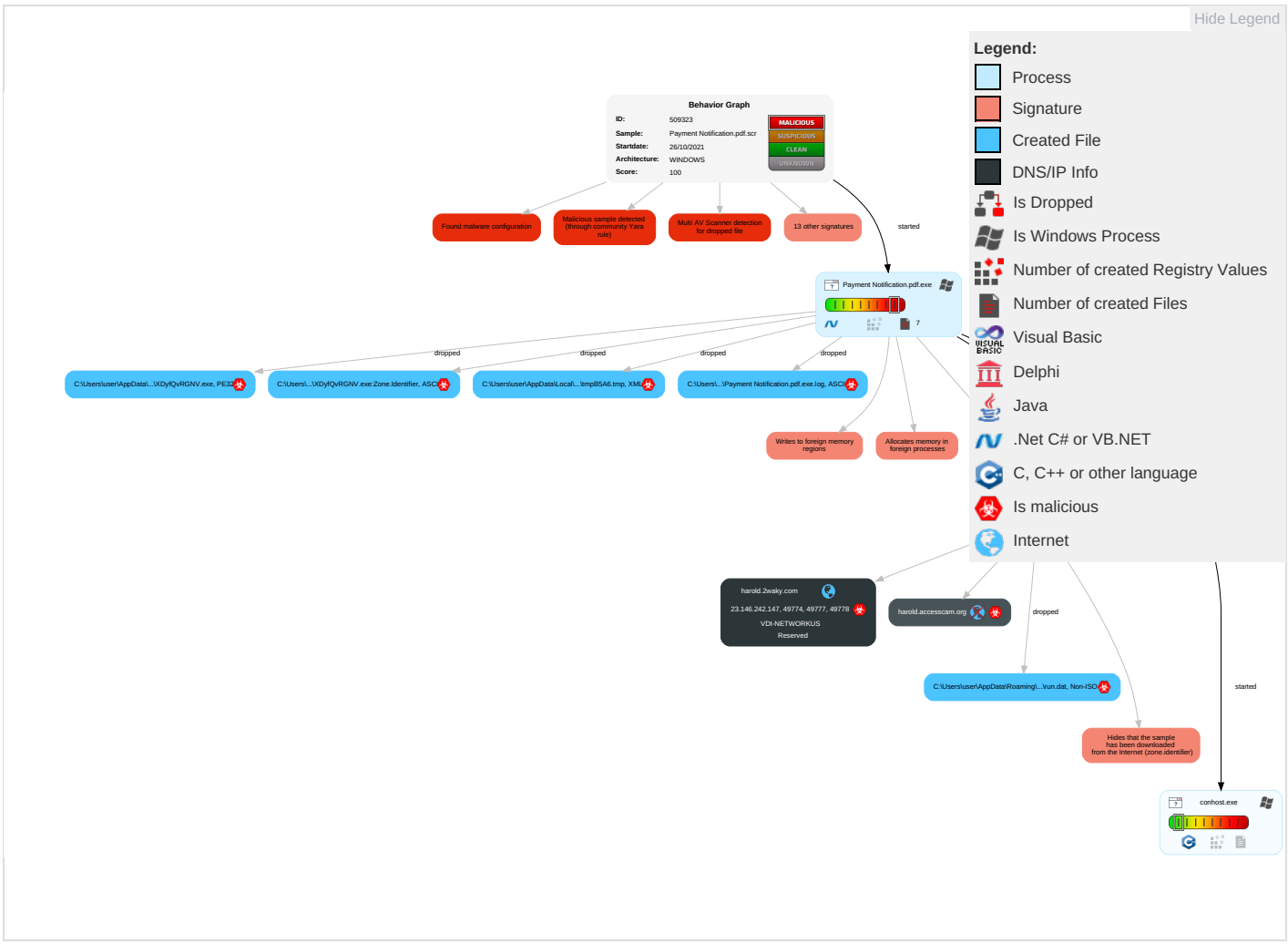
Remote Access Functionality:

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Sta Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicati Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 3	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	File and Directory Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Information Discovery 1 2	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trar Protocol

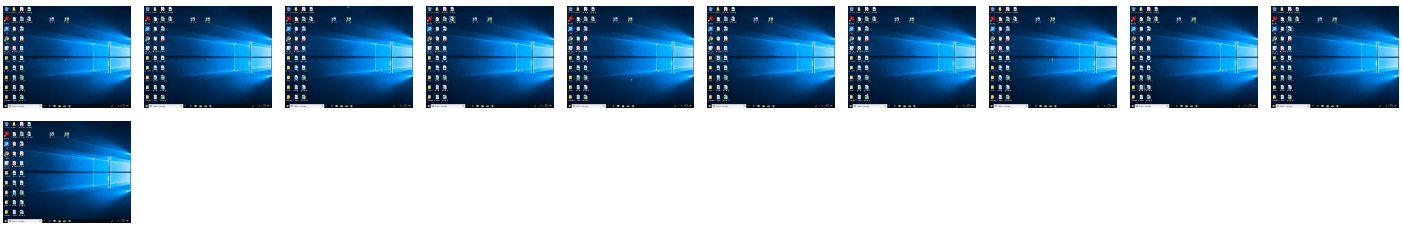
Behavior Graph



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
Payment Notification.pdf.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.APost	
Payment Notification.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\XDyfQvRGNV.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\XDyfQvRGNV.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.APost	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cntte	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTFQ	0%	Avira URL Cloud	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com6	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0z	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.carterandcone.comTCA	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/Kurs	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
harold.accesscam.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/#	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.comles	0%	Avira URL Cloud	safe	
http://www.fontbureau.comnc./t	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comH	0%	URL Reputation	safe	
http://www.founder.com.cn/cnc	0%	URL Reputation	safe	
http://www.founder.com.cn/cne	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/t	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/16	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.carterandcone.com~	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
harold.2waky.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
harold.2waky.com	23.146.242.147	true	true		unknown
harold.accesscam.org	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
harold.accesscam.org	true	• Avira URL Cloud: safe	unknown
harold.2waky.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.146.242.147	harold.2waky.com	Reserved		46664	VDI-NETWORKUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509323
Start date:	26.10.2021
Start time:	12:06:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Notification.pdf.scr (renamed file extension from scr to 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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/9@25/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 0.9%) • Quality average: 36.2% • Quality standard deviation: 38.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:07:35	API Interceptor	2x Sleep call for process: Payment Notification.pdf.exe modified
12:07:39	API Interceptor	940x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.146.242.147	Proof of payment.jpg.exe	Get hash	malicious	Browse	
	HxXHmM0T9f.exe	Get hash	malicious	Browse	
	Payment Notification.exe	Get hash	malicious	Browse	
	Payment Notification.scr.exe	Get hash	malicious	Browse	
	Payment Notification.scr.exe	Get hash	malicious	Browse	
	Request For Quotation.jar	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
harold.2waky.com	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 23.146.242.147
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 185.19.85.137
	Quotation Request.pdf.exe	Get hash	malicious	Browse	• 185.19.85.137
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 185.19.85.137
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	• 185.19.85.137
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	• 185.19.85.137
	HxXHmM0T9f.exe	Get hash	malicious	Browse	• 23.146.242.147
	Request For Quotation.jar	Get hash	malicious	Browse	• 23.146.242.147
	QUOTE.exe	Get hash	malicious	Browse	• 194.5.98.5
	Payment proof.jpg.exe	Get hash	malicious	Browse	• 194.5.98.5
	Proof Of Payment.jpg.exe	Get hash	malicious	Browse	• 194.5.98.5
	Proof of payment.pdf.exe	Get hash	malicious	Browse	• 194.5.98.5
	Payment.pdf.exe	Get hash	malicious	Browse	• 91.193.75.29
	Payment Confirmation.exe	Get hash	malicious	Browse	• 185.165.153.213

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VDI-NETWORKUS	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 23.146.242.147
	7WVpng6phO.exe	Get hash	malicious	Browse	• 156.96.151.237
	hWA2wujmoe.exe	Get hash	malicious	Browse	• 23.146.242.85
	1gPmnCR2PX.exe	Get hash	malicious	Browse	• 23.146.242.85
	bvngnTeTxp.exe	Get hash	malicious	Browse	• 23.146.242.85
	ABzm98MbSD.exe	Get hash	malicious	Browse	• 23.146.242.85
	7w2oGjbrQR.exe	Get hash	malicious	Browse	• 23.146.242.85
	5HpbqZ5r7t.exe	Get hash	malicious	Browse	• 23.146.242.85
	Cu4ltshF0q	Get hash	malicious	Browse	• 156.96.155.230
	RX2dMHNrPL.exe	Get hash	malicious	Browse	• 23.146.242.85
	tZz20galQf.exe	Get hash	malicious	Browse	• 23.146.242.85
	0r22uNk4EF.exe	Get hash	malicious	Browse	• 23.146.242.85
	WbE13U2I1M.exe	Get hash	malicious	Browse	• 23.146.242.85
	DW1VgsgHNU.exe	Get hash	malicious	Browse	• 23.146.242.85
	8TEZmAEx3U.exe	Get hash	malicious	Browse	• 23.146.242.85
	7HHrcwZjLI.exe	Get hash	malicious	Browse	• 23.146.242.85
	466XoziOLD.exe	Get hash	malicious	Browse	• 23.146.242.85
	hVlpEajfIR.exe	Get hash	malicious	Browse	• 23.146.242.85
	0rUkHCgvVf.exe	Get hash	malicious	Browse	• 23.146.242.85
	HxXHmM0T9f.exe	Get hash	malicious	Browse	• 23.146.242.147

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Payment Notification.pdf.exe.log	
Process:	C:\Users\user\Desktop\Payment Notification.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpB5A6.tmp	
Process:	C:\Users\user\Desktop\Payment Notification.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191361547203692
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGVtn:cbhK79lNQR/rydbz9l3YODOLNdq30
MD5:	2F47475C4B4B087C7AA31D5961650D4B
SHA1:	49765D299736594A59E380F27ABCB14ADBD9E2DA
SHA-256:	DD928D2AA2EC67114437376422EE33C321FA972EF4EF6623BE067427178AE1DD
SHA-512:	D1B70CA43C987DFA63C10CA5E3BC39A7488CAE701C2D1F80580BD0F097FCAABE8434071C90C8D4F6EAD127B9C19C2DE7B38EC95429D866E9284901C8CE491 92
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:dNet:Py
MD5:	4AC1BB475FF573310BF15DC6C31BC846
SHA1:	987F6E543C60DE91F724DF5336089FDB7677BF5A
SHA-256:	07BA14A62BF8EEF8FA8B3BBDD6DD398099EFCAC9039ADDB2F104BEB381CC769A
SHA-512:	45429609143113A18120A8C62AFD9E81B9100E8B381596A94049AD9709404B2E00F71CB1A7894DA1A82EDD4226E7E07CE84B99917309A054A95837EC78C98251
Malicious:	**true**
Reputation:	low
Preview:	.TYqh..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:....L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.l,...u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\XDyfQvRGNV.exe	
Process:	C:\Users\user\Desktop\Payment Notification.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	457728
Entropy (8bit):	7.631882884601436
Encrypted:	false
SSDEEP:	6144:75UiswNkTzNaIaX++UCEbOUPhM2yXJogC6HVcUGDneVy2vakl3V:FkyX+7OUPh3y5D1cVDneVyYagV
MD5:	06E79CB697E436C1E66C49D3C39DBD82
SHA1:	025758750EF682CEAD7C98F6CF4156C7BB33A3B2
SHA-256:	07749072A852C769FAD91C350E6921B811FB04DE3448516E2CCF5B81D07E22E7
SHA-512:	F2EC81462399525595B8B0210024E80DA782E09F43DAE71156E5567B590C30FC5716218441664E4E142DBD0F2EC888E78706A20466866814A8D4454423B4BE32
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.wa.....0.....L..... .....@.. .....`..... ..@.....O.....J.....@..... ..... ..H.....text..... ..... ..`.rsrc....J.....J.....@..@.rel oc.....@.....@..B.....H.....?...A.....}.....(J.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0..8.....s....%. Bo.....%.Po.....%.Do.....%.Io.....%.Wo.....+..*.0..8.....s....%.oo.....%.+o.....%.-o.....%.*o.....%.=o.....+..*"..(.....*....0.. .....%.r...p.%.r/..p.%....+..*&.(.....*...0..0.....o# ....oO...3..o%....oQ.....+....,....+....+..*.0..0.....o#....o#...3..o%....o%.....+....,....+....

C:\Users\user\AppData\Roaming\XDyfQvRGNV.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment Notification.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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.631882884601436
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:	Payment Notification.pdf.exe
File size:	457728
MD5:	06e79cb697e436c1e66c49d3c39dbd82
SHA1:	025758750ef682cead7c98f6cf4156c7bb33a3b2
SHA256:	07749072a852c769fad91c350e6921b811fb04de3448516e2ccf5b81d07e22e7
SHA512:	f2ec81462399525595b8b0210024e80da782e09f43dae71156e5567b590c30fc5716218441664e4e142dbd0f2ec888e78706a20466866814a8d4454423b4be32
SSDEEP:	6144:75UiswNkTzNaIaX++UCEbOUPhM2yXJogC6HVcUGDneVy2vakl3V:FkyX+7OUPh3y5D1cVDneVyYagV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.wa.....0.....L..... .....@.. .....`.....@.....

File Icon

Icon Hash:	c4d2c4dcf4c6f230

Static PE Info

General

Entrypoint:	0x45cc02
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:	0x6177B028 [Tue Oct 26 07:37:12 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0x5ac08	0x5ae00	False	0.962613909904	data	7.95381107264	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x14a00	0x14a00	False	0.168276515152	data	4.56109890567	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 26, 2021 12:07:41.512943029 CEST	192.168.2.4	8.8.8.8	0x3b6a	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:41.693167925 CEST	192.168.2.4	8.8.4.4	0x714a	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:41.741597891 CEST	192.168.2.4	8.8.8.8	0x965e	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:45.845683098 CEST	192.168.2.4	8.8.8.8	0x659f	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:45.932966948 CEST	192.168.2.4	8.8.4.4	0x2815	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:45.958858013 CEST	192.168.2.4	8.8.8.8	0xf936	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:50.216686964 CEST	192.168.2.4	8.8.8.8	0x2905	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:50.239002943 CEST	192.168.2.4	8.8.4.4	0x50cc	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:50.266953945 CEST	192.168.2.4	8.8.8.8	0xb3ec	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:54.330153942 CEST	192.168.2.4	8.8.8.8	0xab78	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:00.544697046 CEST	192.168.2.4	8.8.8.8	0x2f90	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:08.555134058 CEST	192.168.2.4	8.8.8.8	0x70bf	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:14.900113106 CEST	192.168.2.4	8.8.8.8	0x4e1a	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:21.499331951 CEST	192.168.2.4	8.8.8.8	0x2154	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:29.199875116 CEST	192.168.2.4	8.8.8.8	0x59b0	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:36.523969889 CEST	192.168.2.4	8.8.8.8	0x696	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:43.741024971 CEST	192.168.2.4	8.8.8.8	0x971f	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:49.903099060 CEST	192.168.2.4	8.8.8.8	0x3abc	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:55.849997044 CEST	192.168.2.4	8.8.8.8	0x31e	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:02.073508024 CEST	192.168.2.4	8.8.8.8	0xc552	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:08.520137072 CEST	192.168.2.4	8.8.8.8	0x383d	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:14.489131927 CEST	192.168.2.4	8.8.8.8	0x711	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:20.514698029 CEST	192.168.2.4	8.8.8.8	0x11a0	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:26.475930929 CEST	192.168.2.4	8.8.8.8	0xe1df	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:32.497100115 CEST	192.168.2.4	8.8.8.8	0x6e77	Standard query (0)	harold.2way.com	A (IP address)	IN (0x0001)

DNS Answers

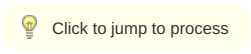
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 12:07:41.531513929 CEST	8.8.8.8	192.168.2.4	0x3b6a	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:41.711807013 CEST	8.8.4.4	192.168.2.4	0x714a	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:41.760184050 CEST	8.8.8.8	192.168.2.4	0x965e	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:45.864526987 CEST	8.8.8.8	192.168.2.4	0x659f	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:45.951548100 CEST	8.8.4.4	192.168.2.4	0x2815	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:45.976881027 CEST	8.8.8.8	192.168.2.4	0xf936	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:50.235449076 CEST	8.8.8.8	192.168.2.4	0x2905	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 26, 2021 12:07:50.257596970 CEST	8.8.4.4	192.168.2.4	0x50cc	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:50.285274029 CEST	8.8.8.8	192.168.2.4	0xb3ec	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 26, 2021 12:07:54.351468086 CEST	8.8.8.8	192.168.2.4	0xab78	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:00.565524101 CEST	8.8.8.8	192.168.2.4	0x2f90	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:08.573555946 CEST	8.8.8.8	192.168.2.4	0x70bf	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:14.916676998 CEST	8.8.8.8	192.168.2.4	0x4e1a	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:21.515520096 CEST	8.8.8.8	192.168.2.4	0x2154	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:29.218661070 CEST	8.8.8.8	192.168.2.4	0x59b0	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:36.540235043 CEST	8.8.8.8	192.168.2.4	0x696	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:43.761434078 CEST	8.8.8.8	192.168.2.4	0x971f	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:49.921401024 CEST	8.8.8.8	192.168.2.4	0x3abc	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:08:55.868859053 CEST	8.8.8.8	192.168.2.4	0x31e	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:02.092452049 CEST	8.8.8.8	192.168.2.4	0xc552	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:08.541229010 CEST	8.8.8.8	192.168.2.4	0x383d	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:14.509752989 CEST	8.8.8.8	192.168.2.4	0x711	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:20.533269882 CEST	8.8.8.8	192.168.2.4	0x11a0	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:26.494824886 CEST	8.8.8.8	192.168.2.4	0xe1df	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)
Oct 26, 2021 12:09:32.521940947 CEST	8.8.8.8	192.168.2.4	0x6e77	No error (0)	harold.2waky.com		23.146.242.147	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment Notification.pdf.exe PID: 6132 Parent PID: 6520

General

Start time:	12:07:30
Start date:	26/10/2021
Path:	C:\Users\user\Desktop\Payment Notification.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Notification.pdf.exe'
Imagebase:	0x960000
File size:	457728 bytes
MD5 hash:	06E79CB697E436C1E66C49D3C39DBD82
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: 00000000.00000002.681190398.0000000003001000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.681509296.0000000004001000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.681509296.0000000004001000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.681509296.0000000004001000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3740 Parent PID: 6132

General

Start time:	12:07:37
Start date:	26/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XDyfQvRGNV' /XML 'C:\Users\user\AppData\Local\Temp\tmpB5A6.tmp'
Imagebase:	0x1390000
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

Analysis Process: conhost.exe PID: 4720 Parent PID: 3740

General

Start time:	12:07:38
Start date:	26/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5412 Parent PID: 6132

General

Start time:	12:07:38
Start date:	26/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xa10000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis