ID: 501103
Sample Name: Proof of payment.jpg.scr
Cookbook: default.jbs
Time: 15:08:19
Date: 12/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report Proof of payment.jpg.scr

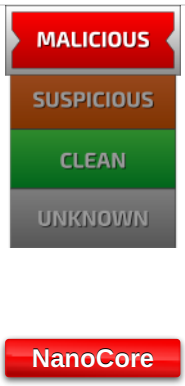
Overview

General Information

Sample Name:	Proof of payment.jpg.scr (renamed file extension from scr to exe)
Analysis ID:	501103
MD5:	f16a886b0c04454.
SHA1:	47ed9cbe0c0430..
SHA256:	9f4c690fdf0c329…
Tags:	exe nanocore
Infos:	

Most interesting Screenshot:

Detection

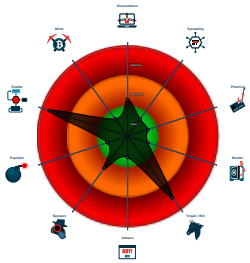


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Multi AV Scanner detection for doma…
- 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…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



- **System is w10x64**
- Proof of payment.jpg.exe (PID: 2940 cmdline: 'C:\Users\user\Desktop\Proof of payment.jpg.exe' MD5: F16A886B0C04454901AC6D0923297C0E)
  - schtasks.exe (PID: 5080 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eoPqnTxJGg' /XML 'C:\Users\user\AppData\Local\Temp\tmpB6E9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 2600 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
00000000.00000002.260682862.00000000028D7000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.260632599.00000000028A1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.261006592.00000000038A1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf3595:$x1: NanoCore.ClientPluginHost • 0x125db5:$x1: NanoCore.ClientPluginHost • 0xf35d2:$x2: IClientNetworkHost • 0x125df2:$x2: IClientNetworkHost • 0xf7105:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x129925:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.261006592.00000000038A1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.261006592.00000000038A1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf32fd:$a: NanoCore • 0xf330d:$a: NanoCore • 0xf3541:$a: NanoCore • 0xf3555:$a: NanoCore • 0xf3595:$a: NanoCore • 0x125b1d:$a: NanoCore • 0x125b2d:$a: NanoCore • 0x125d61:$a: NanoCore • 0x125d75:$a: NanoCore • 0x125db5:$a: NanoCore • 0xf335c:$b: ClientPlugin • 0xf355e:$b: ClientPlugin • 0xf359e:$b: ClientPlugin • 0x125b7c:$b: ClientPlugin • 0x125d7e:$b: ClientPlugin • 0x125dbe:$b: ClientPlugin • 0xf3483:$c: ProjectData • 0x125ca3:$c: ProjectData • 0x202a9e:$c: ProjectData • 0x27d2be:$c: ProjectData • 0xf3e8a:$d: DESCrypto

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.Proof of payment.jpg.exe.3984408.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Proof of payment.jpg.exe.3984408.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$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.Proof of payment.jpg.exe.3984408.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Proof of payment.jpg.exe.3984408.2.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
0.2.Proof of payment.jpg.exe.28a9640.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 3 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 domain / URL
- Yara detected Nanocore RAT

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

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:

- 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

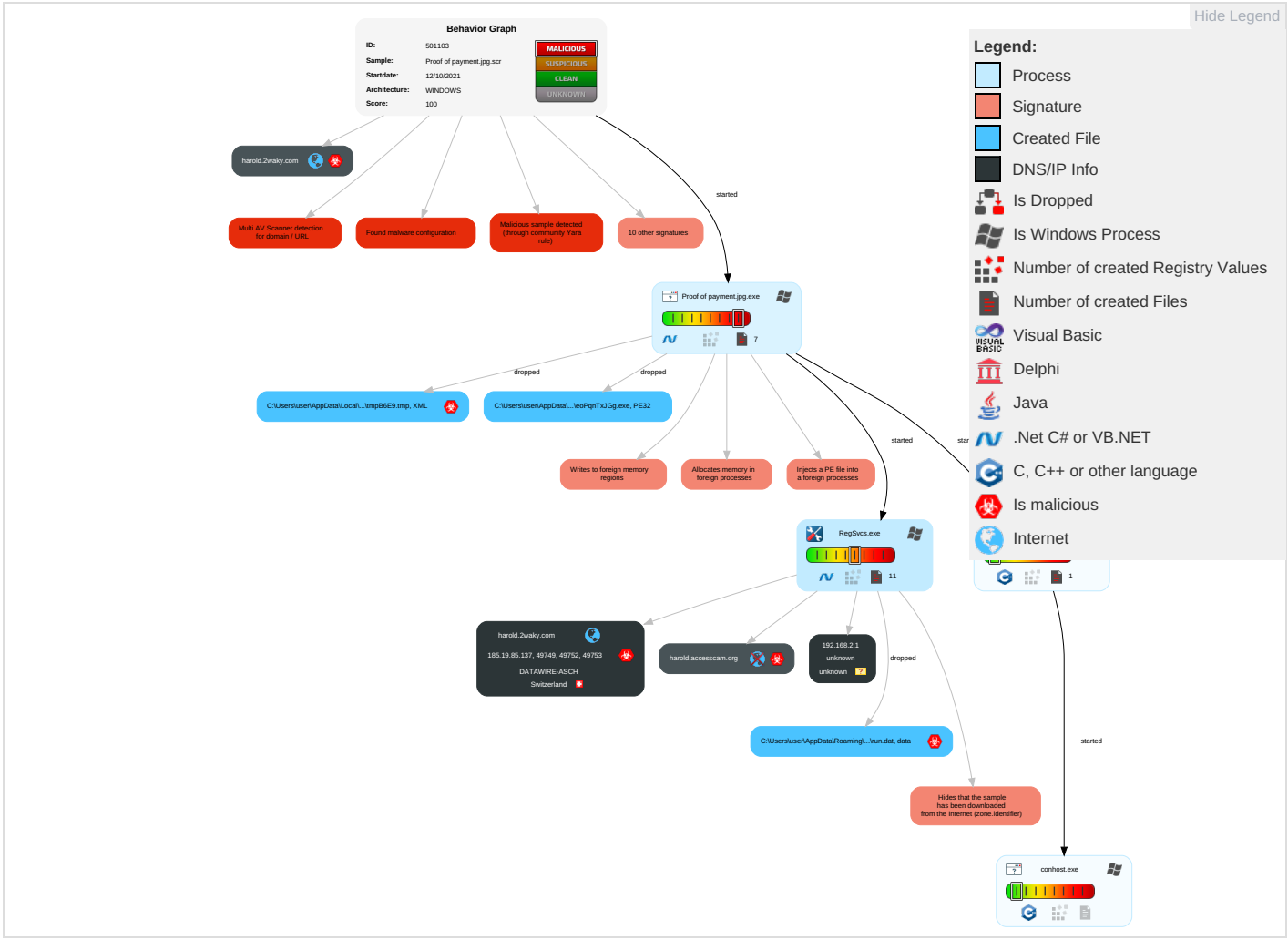
Remote Access Functionality:

- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1 1	Input Capture 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Networ Commu
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
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	Non-Application Layer Protocol 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
harold.2waky.com	15%	Virustotal		Browse
harold.accesscam.org	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comB.TTFK	0%	Avira URL Cloud	safe	
http://www.tiro.comymP	0%	Avira URL Cloud	safe	
http://www.fonts.commN	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sandoll.co.kr2011	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnX	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/-tR	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.com-d	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.commN	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	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/v	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0eb	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.tiro.comj	0%	Avira URL Cloud	safe	
harold.accesscam.org	0%	Avira URL Cloud	safe	
harold.2waky.com	0%	Avira URL Cloud	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.sandoll.co.krlearn	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cne	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
harold.2waky.com	185.19.85.137	true	true	• 15%, Virustotal, Browse	unknown
harold.accesscam.org	unknown	unknown	true	• 5%, Virustotal, Browse	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
185.19.85.137	harold.2waky.com	Switzerland		48971	DATAWIRE-ASCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501103
Start date:	12.10.2021
Start time:	15:08:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proof of payment.jpg.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/8@25/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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
15:09:23	API Interceptor	1x Sleep call for process: Proof of payment.jpg.exe modified
15:09:27	API Interceptor	933x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.19.85.137	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	
	PROFORMA INVOICE 20210823.pdf.exe	Get hash	malicious	Browse	
	New Proforma Invoice20210630.xlxs.exe	Get hash	malicious	Browse	
	Proforma Invoice20210625.pdf.exe	Get hash	malicious	Browse	
	PcdEZG6zDS.exe	Get hash	malicious	Browse	
	sfTZCyMKuC.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
harold.2waky.com	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
DATAWIRE-ASCH	MT103 10.11.pdf.exe	Get hash	malicious	Browse	• 185.19.85.136
	dAkJsQr7A9.exe	Get hash	malicious	Browse	• 185.19.85.175
	GIV PO 00254.xls.exe	Get hash	malicious	Browse	• 185.19.85.136
	dUzAkYsvl8.exe	Get hash	malicious	Browse	• 185.19.85.175
	BL & INVOICE.exe	Get hash	malicious	Browse	• 185.19.85.171
	Routing Details.vbs	Get hash	malicious	Browse	• 185.19.85.170
	Nueva orden #7624.xls.exe	Get hash	malicious	Browse	• 185.19.85.136
	voo7b2BBq6.exe	Get hash	malicious	Browse	• 185.19.85.175
	xmsGPH324z.exe	Get hash	malicious	Browse	• 185.19.85.175
	dVWsghK4Aj.exe	Get hash	malicious	Browse	• 185.19.85.175
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	• 185.19.85.137
	ShippingDocs.exe	Get hash	malicious	Browse	• 185.19.85.171
	2E9xpfvD2O.exe	Get hash	malicious	Browse	• 185.19.85.175
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	• 185.19.85.137
	uF74GlbXPc.exe	Get hash	malicious	Browse	• 185.19.85.175
	jFjTeUfek3.exe	Get hash	malicious	Browse	• 185.19.85.175
	Q7DYDgQhKp.exe	Get hash	malicious	Browse	• 185.19.85.175
	USD31000.exe	Get hash	malicious	Browse	• 185.19.85.171
	32000USD_Swift.exe	Get hash	malicious	Browse	• 185.19.85.171
	dIDGpRFSEo.exe	Get hash	malicious	Browse	• 185.19.85.175

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Proof of payment.jpg.exe.log	
Process:	C:\Users\user\Desktop\Proof of payment.jpg.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:	false
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\tmpB6E9.tmp	
Process:	C:\Users\user\Desktop\Proof of payment.jpg.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.171887955431004
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBetn:cbhC7ZlNQF/rydbz9I3YODOLNdq3C
MD5:	1358393D4D1CFCCE7BD6823A860F20B2
SHA1:	E513A17C19EB5C677435DC73C2533D2A7C52B59F
SHA-256:	66F6CF12179F5F9B8305C4A927D4084B553D9E90166D0D1B1056925D34A9B982
SHA-512:	DA7612128A91DA3B7EA8FB4571F99ACF2BC3BEC2ACD99A2EB73EC563DE9BD2349B8C7CF4A93A8389A6778D0C1537D8ECED2FF8DD6580AA8D506ADDDB69B7 AE04
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	1392
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	24:IQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4l:IknjhUknjhUknjhUknjhUknjhL
MD5:	5E3C10DCF7AAB1A5E4671C3AD52D9BD2
SHA1:	7DE7F5ACAED711BC35E62756D1440E80262D85D1
SHA-256:	B9EB9E732F6204735FFB2C9A6EC8F077E4B4F31E57E336199D22278EAD8412F9
SHA-512:	00252F19A1D0098FEBC78231182FAD57A66390077C0C462C94950D7CA02D53A7B7D692B4D7E718DF2708C1F7919CCB29837A2309E3BEFD2D585FF0C049E5FEB
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......[.&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......[.&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......[.&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......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

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:	data

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:98:y
MD5:	108FC92C1878B6BB04738FB9430AD1A0
SHA1:	030EF679702BA4AC7629B9D6D3980231F35CE18C
SHA-256:	FB9CF8B94C82519C911F1EE89763BF9EDFE05EAC3FDBF7A09229E6BE9AD2DCE2
SHA-512:	1C39811250792C91A1418A424081A627D5032F33F90B3B37EC24824E4BD040EC36C197C628C13B700F6435164339DE77CFB8497476A9E16B4760AF9ECC85A823
Malicious:	**true**
Reputation:	low
Preview:	.....H

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
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.I,....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\eoPqnTxJGg.exe	
Process:	C:\Users\user\Desktop\Proof of payment.jpg.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	686080
Entropy (8bit):	7.645401121666266
Encrypted:	false
SSDEEP:	12288:6MbSB2Fio+a+k09R8Yrt2JX6RaaALVlQ9UfHRkkPG0r5PSsPa23rEG0r5FbnVe:6JBcio+a+ki3VRaaALPhfHRtPG0rpSsQ
MD5:	F16A886B0C04454901AC6D0923297C0E
SHA1:	47ED9CBE0C0430444FFD842A231C06A258FE6A5D
SHA-256:	9F4C690FDF0C329B419EB7CBF02C874DD7BE5EC7BB3585A0C94A0ABA266604D4
SHA-512:	E60A04F86083603CAC82F970552C0031FD52A9CBC7293BA873427D45FBEDFEB13284126BF28EB01692B9C4DA81B26D9146DB7C9F6630A2455E9F32D15183CAE
Malicious:	false

C:\Users\user\AppData\Roaming\eoPqnTxJGg.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....iea.....0..... ... .@.. ....@.....O.... .. ..H.....text..... ....`.rsrc... ....@..@.reloc..... .....v.....@..B.....H.....,_...P.....}.....U.....0..4.....K.....r...p...r...p.....,.....+.....+..*.0..F.....+6.....o.....,.r!..ps....z..X....i....-.*...0..d.....+N..+8.....(.....(.....o.....,r!..ps....z..X....o.....-...X....o.....-.*.0.....+j..+R..+:.....(.....(.....o.....,r!..ps....z..X....o.. .....-...X....o.....-...X....o.....-.*".(.....

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.645401121666266
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Proof of payment.jpg.exe
File size:	686080
MD5:	f16a886b0c04454901ac6d0923297c0e
SHA1:	47ed9cbe0c0430444ffd842a231c06a258fe6a5d
SHA256:	9f4c690fdf0c329b419eb7cbf02c874dd7be5ec7bb3585a0c94a0aba266604d4
SHA512:	e60a04f86083603cac82f970552c0031fd52a9cbc7293ba873427d45fbedfeb13284126bf28eb01692b9c4da81b26d9146db7c9f6630a2455e9f32d15183caeb
SSDEEP:	12288:6MbSB2Fio+a+k09R8Yrt2JX6RaaALVlQ9UfHRkkPG0r5PSsPa23rEG0r5FbnVe:6JBcio+a+ki3VRaaALPhfHRtPG0rpSsQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....iea.....0..... ... .@.. .....@.....

File Icon

Icon Hash:	0089c5cd91810189

Static PE Info

General

Entrypoint:	0x49052e
Entrypoint Section:	.text
Digitally signed:	false

General

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:	0x616569F4 [Tue Oct 12 10:56:52 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	0x8e61c	0x8e800	False	0.924275287829	data	7.85777209159	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x92000	0x18a20	0x18c00	False	0.377426609848	data	5.45184475744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.0815394123432	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 12, 2021 15:09:28.581779003 CEST	192.168.2.5	8.8.8.8	0x63f8	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:28.994478941 CEST	192.168.2.5	8.8.4.4	0x5a24	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:29.297355890 CEST	192.168.2.5	8.8.8.8	0x1570	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:34.137134075 CEST	192.168.2.5	8.8.8.8	0x27a7	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:34.171382904 CEST	192.168.2.5	8.8.4.4	0xe05e	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:34.248856068 CEST	192.168.2.5	8.8.8.8	0x9cfa	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:38.479859114 CEST	192.168.2.5	8.8.8.8	0x5fc4	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 12, 2021 15:09:38.502695084 CEST	192.168.2.5	8.8.4.4	0x3e9	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:38.531282902 CEST	192.168.2.5	8.8.8.8	0xe842	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:42.769747019 CEST	192.168.2.5	8.8.8.8	0xd004	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:49.097486973 CEST	192.168.2.5	8.8.8.8	0x733e	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:56.914613962 CEST	192.168.2.5	8.8.8.8	0xf51f	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:03.356395960 CEST	192.168.2.5	8.8.8.8	0xb9a8	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:09.863465071 CEST	192.168.2.5	8.8.8.8	0xf5aa	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:16.205543041 CEST	192.168.2.5	8.8.8.8	0x71da	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:22.732084036 CEST	192.168.2.5	8.8.8.8	0x2831	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:29.331429958 CEST	192.168.2.5	8.8.8.8	0x85d4	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:36.415932894 CEST	192.168.2.5	8.8.8.8	0xa351	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:42.501702070 CEST	192.168.2.5	8.8.8.8	0x5457	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:48.522980928 CEST	192.168.2.5	8.8.8.8	0xefe	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:54.661490917 CEST	192.168.2.5	8.8.8.8	0xbbcb	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:00.709645033 CEST	192.168.2.5	8.8.8.8	0x5fe1	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:06.779176950 CEST	192.168.2.5	8.8.8.8	0xe098	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:14.627098083 CEST	192.168.2.5	8.8.8.8	0x9026	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:20.681814909 CEST	192.168.2.5	8.8.8.8	0xa277	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 15:09:28.717128992 CEST	8.8.8.8	192.168.2.5	0x63f8	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:29.173227072 CEST	8.8.4.4	192.168.2.5	0x5a24	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:29.320130110 CEST	8.8.8.8	192.168.2.5	0x1570	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:34.156547070 CEST	8.8.8.8	192.168.2.5	0x27a7	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:34.189163923 CEST	8.8.4.4	192.168.2.5	0xe05e	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:34.423072100 CEST	8.8.8.8	192.168.2.5	0x9cfa	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:38.496443987 CEST	8.8.8.8	192.168.2.5	0x5fc4	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:38.521024942 CEST	8.8.4.4	192.168.2.5	0x3e9	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:38.549801111 CEST	8.8.8.8	192.168.2.5	0xe842	Name error (3)	harold.acc esscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:42.789721012 CEST	8.8.8.8	192.168.2.5	0xd004	No error (0)	harold.2wa ky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:49.134582043 CEST	8.8.8.8	192.168.2.5	0x733e	No error (0)	harold.2wa ky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:09:56.933176994 CEST	8.8.8.8	192.168.2.5	0xf51f	No error (0)	harold.2wa ky.com		185.19.85.137	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 15:10:03.377588987 CEST	8.8.8.8	192.168.2.5	0xb9a8	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:09.883897066 CEST	8.8.8.8	192.168.2.5	0xf5aa	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:16.224287033 CEST	8.8.8.8	192.168.2.5	0x71da	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:22.750188112 CEST	8.8.8.8	192.168.2.5	0x2831	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:29.350970030 CEST	8.8.8.8	192.168.2.5	0x85d4	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:36.436556101 CEST	8.8.8.8	192.168.2.5	0xa351	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:42.520405054 CEST	8.8.8.8	192.168.2.5	0x5457	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:48.544002056 CEST	8.8.8.8	192.168.2.5	0xefe	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:10:54.678647995 CEST	8.8.8.8	192.168.2.5	0xbbcb	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:00.730202913 CEST	8.8.8.8	192.168.2.5	0x5fe1	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:06.799339056 CEST	8.8.8.8	192.168.2.5	0xe098	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:14.647671938 CEST	8.8.8.8	192.168.2.5	0x9026	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:11:20.989131927 CEST	8.8.8.8	192.168.2.5	0xa277	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Proof of payment.jpg.exe PID: 2940 Parent PID: 5620

General

Start time:	15:09:16
Start date:	12/10/2021
Path:	C:\Users\user\Desktop\Proof of payment.jpg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proof of payment.jpg.exe'
Imagebase:	0x140000

File size:	686080 bytes
MD5 hash:	F16A886B0C04454901AC6D0923297C0E
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: 00000000.00000002.260682862.00000000028D7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.260632599.00000000028A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.261006592.00000000038A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.261006592.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.261006592.00000000038A1000.00000004.00000001.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: 5080 Parent PID: 2940

General

Start time:	15:09:24
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eoPqnTxJGg' /XML 'C:\Users\user\AppData\Local\Temp\tmpB6E9.tmp'
Imagebase:	0x1c0000
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: 4924 Parent PID: 5080

General

Start time:	15:09:25
Start date:	12/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 2600 Parent PID: 2940

General

Start time:	15:09:25
Start date:	12/10/2021
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:	0xd60000
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 Written

File Read

Disassembly

Code Analysis