ID: 501145
Sample Name: Quotation Request.pdf.scr
Cookbook: default.jbs
Time: 15:48:13
Date: 12/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Quotation Request.pdf.scr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 18
DNS Queries 18

DNS Answers 19
Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: Quotation Request.pdf.exe PID: 4556 Parent PID: 5740 20
General 20
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: schtasks.exe PID: 2812 Parent PID: 4556 21
General 21
File Activities 21
Analysis Process: conhost.exe PID: 5048 Parent PID: 2812 21
General 21
Analysis Process: RegSvcs.exe PID: 408 Parent PID: 4556 22
General 22
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Disassembly 22
Code Analysis 22

Windows Analysis Report Quotation Request.pdf.scr

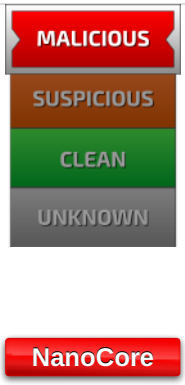
Overview

General Information

Sample Name:	Quotation Request.pdf.scr (renamed file extension from scr to exe)
Analysis ID:	501145
MD5:	95d884c21021e6..
SHA1:	38786584d7caf1b.
SHA256:	b7e4d5626ef15e8.
Tags:	exe nanocore
Infos:	

Most interesting Screenshot:

Detection

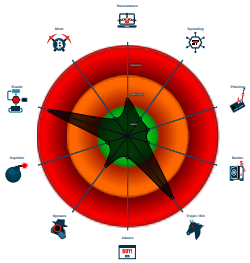


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 doma…
- 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…

Classification



- **System is w10x64**
- Quotation Request.pdf.exe (PID: 4556 cmdline: 'C:\Users\user\Desktop\Quotation Request.pdf.exe' MD5: 95D884C21021E67EA7E9E204A0488FA3)
  - schtasks.exe (PID: 2812 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eqNjYDmhJoX' /XML 'C:\Users\user\AppData\Local\Temp\tmpAC55.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 408 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
00000000.00000002.271877487.0000000002D61000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.271987580.0000000002D97000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.273290959.0000000003D61000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xbc275:$x1: NanoCore.ClientPluginHost • 0xeea95:$x1: NanoCore.ClientPluginHost • 0xbc2b2:$x2: IClientNetworkHost • 0xeead2:$x2: IClientNetworkHost • 0xbfde5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xf2605:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.273290959.0000000003D61000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.273290959.0000000003D61000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xbbfdd:$a: NanoCore • 0xbbfed:$a: NanoCore • 0xbc221:$a: NanoCore • 0xbc235:$a: NanoCore • 0xbc275:$a: NanoCore • 0xee7fd:$a: NanoCore • 0xee80d:$a: NanoCore • 0xeea41:$a: NanoCore • 0xeea55:$a: NanoCore • 0xeea95:$a: NanoCore • 0xbc03c:$b: ClientPlugin • 0xbc23e:$b: ClientPlugin • 0xbc27e:$b: ClientPlugin • 0xee85c:$b: ClientPlugin • 0xeea5e:$b: ClientPlugin • 0xeea9e:$b: ClientPlugin • 0xbc163:$c: ProjectData • 0xee983:$c: ProjectData • 0x1efe33:$c: ProjectData • 0x265653:$c: ProjectData • 0xbcb6a:$d: DESCrypto

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.Quotation Request.pdf.exe.3e0d0e8.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Quotation Request.pdf.exe.3e0d0e8.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$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.Quotation Request.pdf.exe.3e0d0e8.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Quotation Request.pdf.exe.3e0d0e8.2.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.Quotation Request.pdf.exe.2d69644.1.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 submitted file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- 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
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

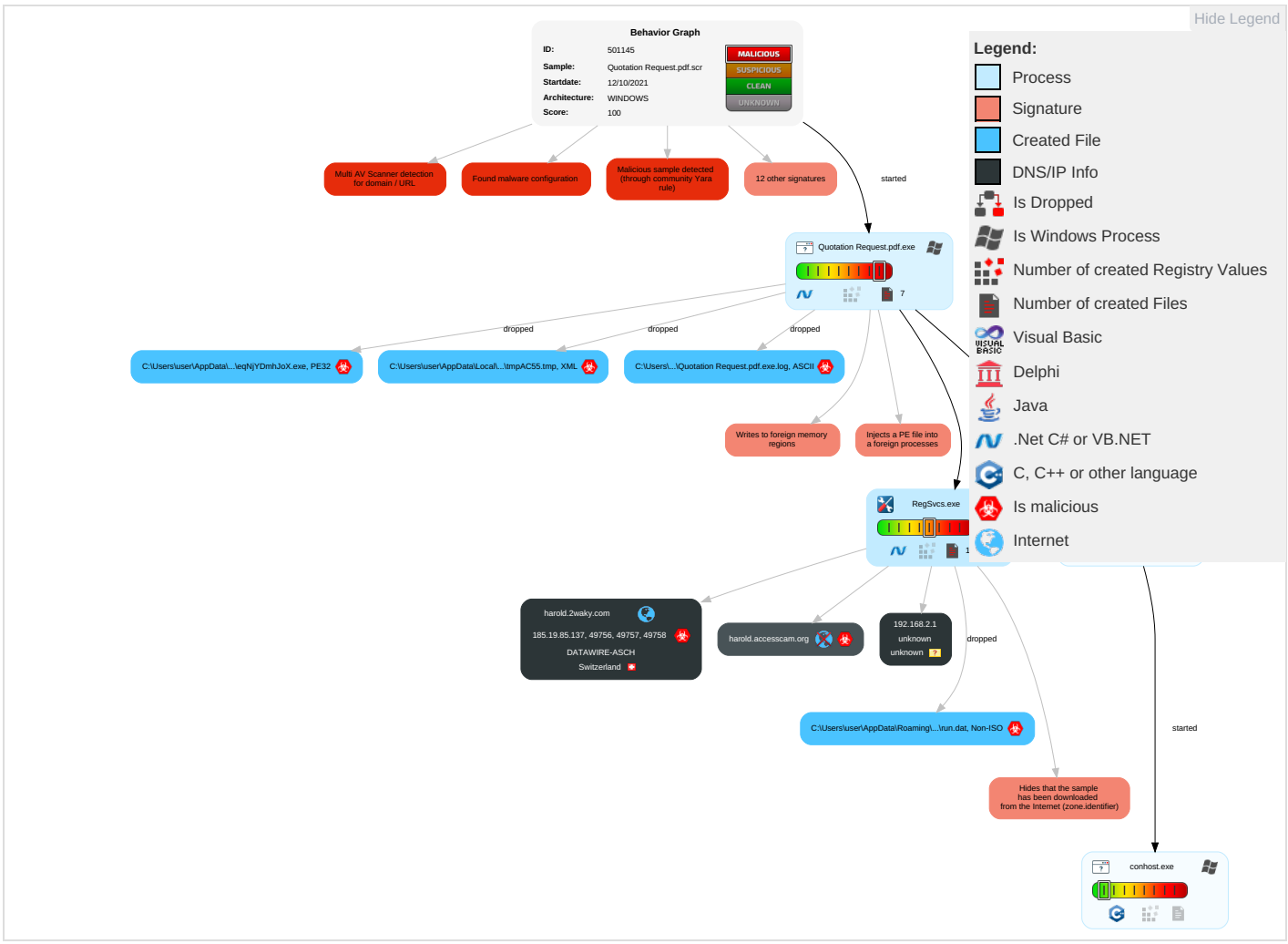
Remote Access Functionality:

- 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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job 1	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-Standard Port 1	Explo Redir Calls/
Domain Accounts	At (Linux)	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-Application Layer Protocol 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM (Swap
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 Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

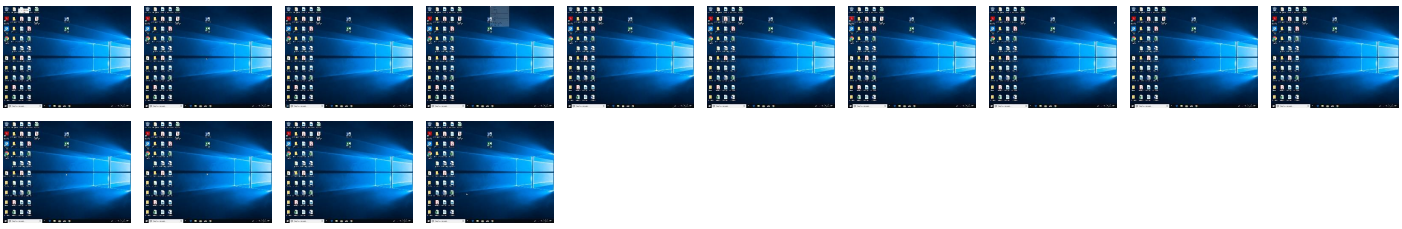
Behavior Graph



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
Quotation Request.pdf.exe	11%	ReversingLabs	ByteCode-MSIL.Trojan.APost	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eqNjYDmhJoX.exe	11%	ReversingLabs	ByteCode-MSIL.Trojan.APost	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
harold.2waky.com	15%	Virustotal		Browse
windowsupdate.s.llnwi.net	0%	Virustotal		Browse
harold.accesscam.org	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmB	0%	Avira URL Cloud	safe	
http://www.tiro.comslnta;	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn5	0%	Avira URL Cloud	safe	
http://www.fonts.com-	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/2	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/9	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	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.jiyu-kobo.co.jp//C	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
harold.accesscam.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0Pq	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnZ	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.comalsk	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/U	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr-cM	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0C	0%	Avira URL Cloud	safe	
http://www.urwpp.deax;	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/ru	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.urwpp.de9;	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma2	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/q	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
harold.2waky.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalic	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
windowsupdate.s.llnwi.net	178.79.242.0	true	false	• 0%, 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:	501145
Start date:	12.10.2021
Start time:	15:48:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation Request.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:	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@6/9@25/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.7%) • Quality average: 70.6% • Quality standard deviation: 36.8%
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
15:49:19	API Interceptor	1x Sleep call for process: Quotation Request.pdf.exe modified
15:49:22	API Interceptor	898x 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.exe	Get hash	malicious	Browse	
	Proof of payment.jpg.exe	Get hash	malicious	Browse	
	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.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
windowsupdate.s.llnwi.net	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 178.79.242.128
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 178.79.242.0
	jjBv8SpZXm.exe	Get hash	malicious	Browse	• 178.79.242.128
	COPIA DE PAGO.exe	Get hash	malicious	Browse	• 178.79.242.0
	Dekont.exe	Get hash	malicious	Browse	• 178.79.242.0
	New Order Inquiry No.96883,pdf.exe	Get hash	malicious	Browse	• 178.79.242.0
	orde443123.exe	Get hash	malicious	Browse	• 178.79.242.128
	Invoice-514777_20211011.xlsb	Get hash	malicious	Browse	• 178.79.242.0
	dorlla.exe	Get hash	malicious	Browse	• 178.79.242.0
	photos jpg.exe	Get hash	malicious	Browse	• 178.79.242.128
	2xYyRwsd4z.exe	Get hash	malicious	Browse	• 178.79.242.0
	client.exe	Get hash	malicious	Browse	• 178.79.242.0
	dAkJsQr7A9.exe	Get hash	malicious	Browse	• 178.79.242.0
	Shipping Documents.exe	Get hash	malicious	Browse	• 178.79.242.0
	preuve de paiement.exe	Get hash	malicious	Browse	• 178.79.242.0
	QUOTATIO.EXE	Get hash	malicious	Browse	• 178.79.242.0
	kR8No6snIq.exe	Get hash	malicious	Browse	• 178.79.242.128
	DHL 299248 AWB 171021.exe	Get hash	malicious	Browse	• 178.79.242.128
	Order_specs_sheet.pdf.jar	Get hash	malicious	Browse	• 178.79.242.0
	pidHTSIGEi8DrAmaYu9K8ghN89.dll	Get hash	malicious	Browse	• 178.79.242.0

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATAWIRE-ASCH	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 185.19.85.137
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 185.19.85.137
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Quotation Request.pdf.exe.log

Process:	C:\Users\user\Desktop\Quotation Request.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\tmpAC55.tmp

Process:	C:\Users\user\Desktop\Quotation Request.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1660
Entropy (8bit):	5.187608923076909
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBPtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3L
MD5:	90ACD9A9C97A5C0E43DA656B494C79A0
SHA1:	911E7AE189E24AC9E7DB82537F186EEE1D1F352F
SHA-256:	8C19DE887CC9B2DBC4D20252D8955274AF48A62DD544096CFC0830AEEC0CA02E

C:\Users\user\AppData\Local\Temp\tmpAC55.tmp

SHA-512:	7A193A28A1B8703D1A0B79401495AB6509A28BC2BB5E318EFAEC63CD2A01D4F50E684E9E5CADF03BA6F63BA233CC2B6C15070C76CD01D430BC0310F35E86B8 DC
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

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+dQnybgC4jh+dQnybgC4l:IknjhUknjhUknjhUknjhUknjhUknjhL
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:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:O1o8tn:OFn
MD5:	EEEF6DA74F6FA0AC71E338AD0B010144
SHA1:	5C7F53209A792A7996DC66C1FB8811FD4D709661
SHA-256:	7C860F32B254485BFAF2BC37A1CC9FF6A90F00CF11BA321E3DD68F0F76E23064
SHA-512:	16C4352D1AF28B0CCFD9B3AE09B27E3080BEF3A0F40B7D1A35227AD2AACE06C17D6F56BDED3C8A477DB449B688512255A886005420D4DF7D892FEFA391B6C5 8
Malicious:	**true**
Reputation:	low
Preview:	-....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):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a........~.~.......3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVnXygY6oRDT6P2bfVn1:RzWDT62DWDT621
MD5:	4315325323A62DE913E5CCD153817BCE
SHA1:	8B38155CD8ACB20BBA0C2A8AF02BFD35B15221A8
SHA-256:	E0C2085D878FDF53CD7D8F0AA9F07490802C51FC3C14A52B6FEA96AD0743C838
SHA-512:	B5036A6CD4852CEBCA86F588D94B9D58B63EB07B2F4DEBD38D5E1BE68B0BB62F82FA239673B6C08F432A28DD50E1D15773DC3738251BD2F9959F1255D72745B
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.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..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=.....L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!.:.^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\eqNjYDmhJoX.exe	
Process:	C:\Users\user\Desktop\Quotation Request.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	650240
Entropy (8bit):	7.635016130821497
Encrypted:	false
SSDEEP:	12288:QMySBziJmqgE0pGxgCfZk1LrWkHMlYp6/50jccyQ7w5MV:QMB5b3CfZHkKAA50VdU56
MD5:	95D884C21021E67EA7E9E204A0488FA3
SHA1:	38786584D7CAF1B36E7B72BF85099A82589C48A6
SHA-256:	B7E4D5626EF15E8584E644E1BFAADE75C1FAAA54549BDE7560F44BD3550281DE
SHA-512:	4AF1BF9C684F2AA3DEE982DCA10471FB912744385FE9567039BAF7109E51D70F85D3023544A0AC83595D73968406B8C269F5EDB59E1B9E8FCF96759549529BFD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*ea.....0.....L..... .....@.. .....@..... .@.....O.....H..... ....H.....text..... ....`.rsrc....H.....J.....@..@.reloc..... .. .....@..B.....H.....P.....}...`...8.....0..4.....K.....r...p...rC..p.....,.....+.....+..*.0..F.....+6.....o.....,r a..ps....z..X....i....-.*...0..d.....+N..+8.....(.....(.....o.....,ra..ps....z..X....o.....-...X....o.....-.*.0.....+j..+R..+:.....(.....(.....o.....,ra..ps....z..X....o.... .....-...X....o.....-...X....o.....-.*".(.....

C:\Users\user\AppData\Roaming\eqNjYDmhJoX.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Quotation Request.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

C:\Users\user\AppData\Roaming\eqNjYDmhJoX.exe:Zone.Identifier	
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):	7.635016130821497
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:	Quotation Request.pdf.exe
File size:	650240
MD5:	95d884c21021e67ea7e9e204a0488fa3
SHA1:	38786584d7caf1b36e7b72bf85099a82589c48a6
SHA256:	b7e4d5626ef15e8584e644e1bfaade75c1faaa54549bde7560f44bd3550281de
SHA512:	4af1bf9c684f2aa3dee982dca10471fb912744385fe9567039baf7109e51d70f85d3023544a0ac83595d73968406b8c269f5edb59e1b9e8fcf96759549529bfd
SSDEEP:	12288:QMySBziJmqgE0pGxgCfZk1LrWkHMlYp6/50jccyQ7w5MV:QMB5b3CfZHkKAA50VdU56
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....*ea.....0.....L..... .....@.. .....@.....@.....

File Icon

Icon Hash:	c4d2c4dcf4c6f230

Static PE Info

General

Entrypoint:	0x48bcea
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:	0x61652ADD [Tue Oct 12 06:27:41 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	0x89dd8	0x89e00	False	0.922330079896	data	7.85672483308	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x14804	0x14a00	False	0.164701704545	data	4.56196917542	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa2000	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 12, 2021 15:49:25.446805954 CEST	192.168.2.7	8.8.8.8	0xbf69	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:26.437062979 CEST	192.168.2.7	8.8.4.4	0x6768	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:27.565529108 CEST	192.168.2.7	8.8.8.8	0x1a46	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:32.029913902 CEST	192.168.2.7	8.8.8.8	0x6cd3	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:32.403435946 CEST	192.168.2.7	8.8.4.4	0x4e54	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:32.804759026 CEST	192.168.2.7	8.8.8.8	0x90da	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:36.888720989 CEST	192.168.2.7	8.8.8.8	0xe08a	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:37.148696899 CEST	192.168.2.7	8.8.4.4	0x2875	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:37.173485994 CEST	192.168.2.7	8.8.8.8	0xe73c	Standard query (0)	harold.acc esscam.org	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:41.263663054 CEST	192.168.2.7	8.8.8.8	0x4a68	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:47.804738998 CEST	192.168.2.7	8.8.8.8	0x1f17	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:54.211075068 CEST	192.168.2.7	8.8.8.8	0x4f0a	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:00.510494947 CEST	192.168.2.7	8.8.8.8	0xfdac	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:06.939441919 CEST	192.168.2.7	8.8.8.8	0x3176	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:13.268897057 CEST	192.168.2.7	8.8.8.8	0x4488	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:18.193945885 CEST	192.168.2.7	8.8.8.8	0x2614	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:24.683237076 CEST	192.168.2.7	8.8.8.8	0x2389	Standard query (0)	harold.2wa ky.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 12, 2021 15:50:32.143759966 CEST	192.168.2.7	8.8.8.8	0x5e9f	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:38.403631926 CEST	192.168.2.7	8.8.8.8	0x1ccb	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:44.623191118 CEST	192.168.2.7	8.8.8.8	0x1180	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:50.973814011 CEST	192.168.2.7	8.8.8.8	0x9163	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:57.031918049 CEST	192.168.2.7	8.8.8.8	0xb51c	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:51:03.064064026 CEST	192.168.2.7	8.8.8.8	0x702a	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:51:09.126790047 CEST	192.168.2.7	8.8.8.8	0x5fe9	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)
Oct 12, 2021 15:51:16.425517082 CEST	192.168.2.7	8.8.8.8	0xe98a	Standard query (0)	harold.2waky.com	A (IP address)	IN (0x0001)

DNS Answers

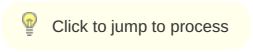
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 15:49:25.466027975 CEST	8.8.8.8	192.168.2.7	0xbf69	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:26.613787889 CEST	8.8.4.4	192.168.2.7	0x6768	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:27.745409966 CEST	8.8.8.8	192.168.2.7	0x1a46	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:32.167773962 CEST	8.8.8.8	192.168.2.7	0x6cd3	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:32.578960896 CEST	8.8.4.4	192.168.2.7	0x4e54	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:32.823015928 CEST	8.8.8.8	192.168.2.7	0x90da	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:37.068095922 CEST	8.8.8.8	192.168.2.7	0xe08a	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:37.166666031 CEST	8.8.4.4	192.168.2.7	0x2875	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:37.191988945 CEST	8.8.8.8	192.168.2.7	0xe73c	Name error (3)	harold.accesscam.org	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:41.282803059 CEST	8.8.8.8	192.168.2.7	0x4a68	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:47.827729940 CEST	8.8.8.8	192.168.2.7	0x1f17	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:54.232299089 CEST	8.8.8.8	192.168.2.7	0x4f0a	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:55.974659920 CEST	8.8.8.8	192.168.2.7	0xec84	No error (0)	windowsupdate.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:55.974659920 CEST	8.8.8.8	192.168.2.7	0xec84	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 12, 2021 15:49:57.063689947 CEST	8.8.8.8	192.168.2.7	0xdf9b	No error (0)	windowsupdate.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:00.530226946 CEST	8.8.8.8	192.168.2.7	0xfdac	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:06.960129023 CEST	8.8.8.8	192.168.2.7	0x3176	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:13.287166119 CEST	8.8.8.8	192.168.2.7	0x4488	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:18.212002993 CEST	8.8.8.8	192.168.2.7	0x2614	No error (0)	harold.2waky.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 15:50:24.701410055 CEST	8.8.8.8	192.168.2.7	0x2389	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:32.162180901 CEST	8.8.8.8	192.168.2.7	0x5e9f	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:38.422909975 CEST	8.8.8.8	192.168.2.7	0x1ccb	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:44.643498898 CEST	8.8.8.8	192.168.2.7	0x1180	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:50.994389057 CEST	8.8.8.8	192.168.2.7	0x9163	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:50:57.050472975 CEST	8.8.8.8	192.168.2.7	0xb51c	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:51:03.086414099 CEST	8.8.8.8	192.168.2.7	0x702a	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:51:09.145246983 CEST	8.8.8.8	192.168.2.7	0x5fe9	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)
Oct 12, 2021 15:51:16.442230940 CEST	8.8.8.8	192.168.2.7	0xe98a	No error (0)	harold.2waky.com		185.19.85.137	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation Request.pdf.exe PID: 4556 Parent PID: 5740

General

Start time:	15:49:10
Start date:	12/10/2021
Path:	C:\Users\user\Desktop\Quotation Request.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation Request.pdf.exe'
Imagebase:	0x640000
File size:	650240 bytes
MD5 hash:	95D884C21021E67EA7E9E204A0488FA3
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: 00000000.00000002.271877487.0000000002D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.271987580.0000000002D97000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.273290959.0000000003D61000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.273290959.0000000003D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.273290959.0000000003D61000.00000004.00000001.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: 2812 Parent PID: 4556

General

Start time:	15:49:20
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\eqNjYDmhJoX' /XML 'C:\Users\user\AppData\Local\Temp\tmpAC55.tmp'
Imagebase:	0xd70000
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: 5048 Parent PID: 2812

General

Start time:	15:49:21
Start date:	12/10/2021
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: RegSvcs.exe PID: 408 Parent PID: 4556

General

Start time:	15:49:21
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:	0x870000
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