ID: 322137
Sample Name: OFFER.exe
Cookbook: default.jbs
Time: 15:27:11
Date: 24/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

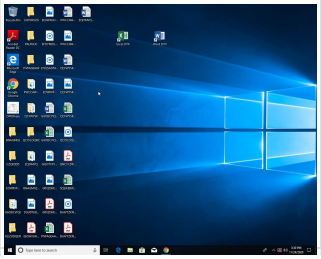
Analysis Report OFFER.exe

Overview

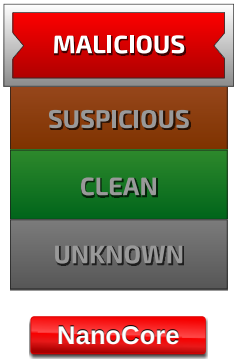
General Information

Sample Name:	OFFER.exe
Analysis ID:	322137
MD5:	f0a3b70a92ece32.
SHA1:	5af0534294c9f5f…
SHA256:	0a09ec08c85008..
Tags:	NanoCore

Most interesting Screenshot:



Detection

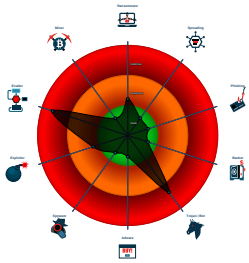


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- OFFER.exe (PID: 6088 cmdline: 'C:\Users\user\Desktop\OFFER.exe' MD5: F0A3B70A92ECE3204289B3E1E25C9942)
  - schtasks.exe (PID: 5436 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RplepwTnfZYE' /XML 'C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - OFFER.exe (PID: 5056 cmdline: C:\Users\user\Desktop\OFFER.exe MD5: F0A3B70A92ECE3204289B3E1E25C9942)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.210666466.0000000002EA1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.211065928.0000000003EA1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1116cd:$x1: NanoCore.ClientPluginHost • 0x143eed:$x1: NanoCore.ClientPluginHost • 0x11170a:$x2: IClientNetworkHost • 0x143f2a:$x2: IClientNetworkHost • 0x11523d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x147a5d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.211065928.0000000003EA1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.211065928.0000000003EA1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x111435:$a: NanoCore • 0x111445:$a: NanoCore • 0x111679:$a: NanoCore • 0x11168d:$a: NanoCore • 0x1116cd:$a: NanoCore • 0x143c55:$a: NanoCore • 0x143c65:$a: NanoCore • 0x143e99:$a: NanoCore • 0x143ead:$a: NanoCore • 0x143eed:$a: NanoCore • 0x111494:$b: ClientPlugin • 0x111696:$b: ClientPlugin • 0x1116d6:$b: ClientPlugin • 0x143cb4:$b: ClientPlugin • 0x143eb6:$b: ClientPlugin • 0x143ef6:$b: ClientPlugin • 0x1115bb:$c: ProjectData • 0x143ddb:$c: ProjectData • 0x111fc2:$d: DESCrypto • 0x1447e2:$d: DESCrypto • 0x11998e:$e: KeepAlive
00000000.00000002.210800137.0000000002F20000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 1 entries				

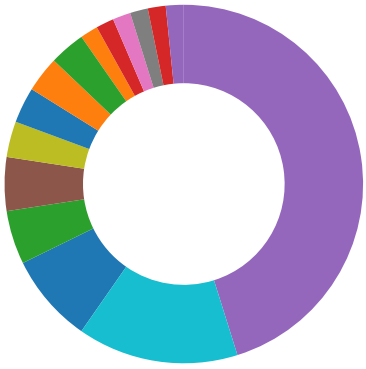
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

- AV Detection
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

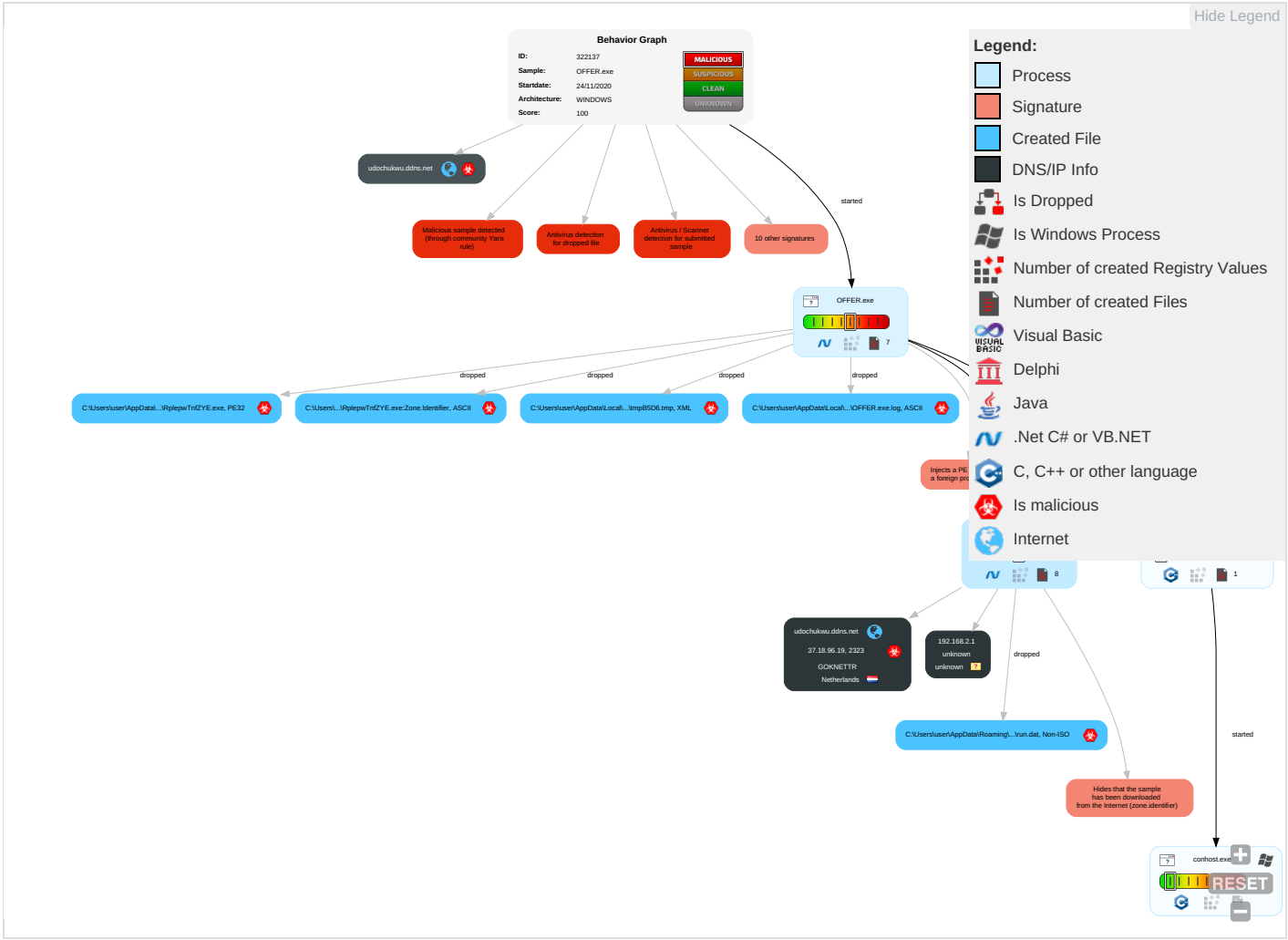
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	System Information Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

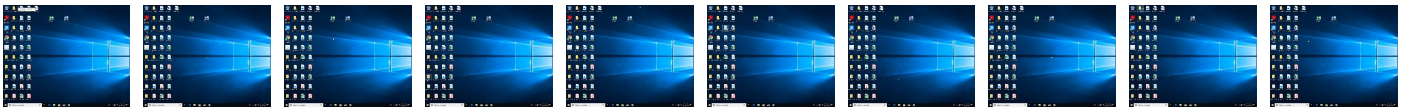
Behavior Graph



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
OFFER.exe	57%	Virustotal		Browse
OFFER.exe	41%	Metadefender		Browse
OFFER.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
OFFER.exe	100%	Avira	TR/AD.Nanocore.gzsda	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	100%	Avira	TR/AD.Nanocore.gzsda	
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	57%	Virustotal		Browse
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	41%	Metadefender		Browse
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
udochukwu.ddns.net	1%	Virustotal		Browse

URLs

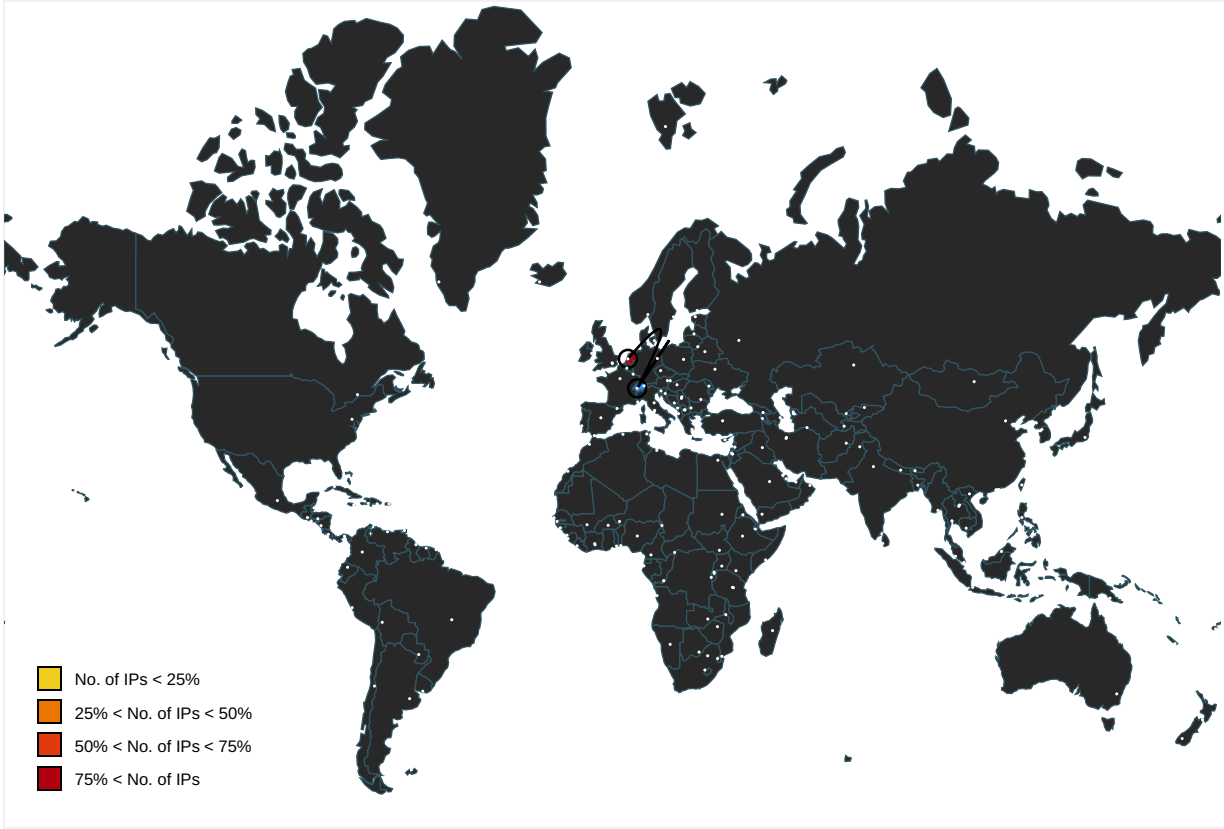
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
udochukwu.ddns.net	37.18.96.19	true	true	• 1%, Virustotal, Browse	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.18.96.19	unknown	Netherlands		201411	GOKNETTR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322137
Start date:	24.11.2020
Start time:	15:27:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OFFER.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@6/5@9/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 13.88.21.125, 51.104.139.180, 92.122.144.200, 20.54.26.129, 8.241.122.126, 8.241.9.254, 67.26.139.254, 8.241.11.254, 8.253.204.121, 92.122.213.247, 92.122.213.194, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:27:58	API Interceptor	1064x Sleep call for process: OFFER.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
udochukwu.ddns.net	xh1V3riWZ5.exe	Get hash	malicious	Browse	• 216.38.8.174
	A2UVQZMMkB.exe	Get hash	malicious	Browse	• 216.38.8.174
	PURCHASE09812.exe	Get hash	malicious	Browse	• 185.140.53.132

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\OFFER.exe.log	
Process:	C:\Users\user\Desktop\OFFER.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:	moderate, 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\tmpB5D6.tmp	
Process:	C:\Users\user\Desktop\OFFER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp	
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.191084760568334
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBPtn:cbh47TlNQ//rydbz9l3YODOLNdq3T
MD5:	AB592D06D98D97E7246ACDE4BC6F877E
SHA1:	6F407D15DCD33272C9F36A3B60CE18EA287D943D
SHA-256:	5F401C9D62E49D3C79957EE747E11E54B09AE2577B37BF3FD8E0F59779E17764
SHA-512:	323FEB7A1596BC5CCC43507EC2D975930D4A35E9D726592570FD27CA47874336CB1743BC9F2E4E0BF4A32FA9605280B27281E373F176AE3762E1F33B50EE5BCI
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\run.dat	
Process:	C:\Users\user\Desktop\OFFER.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:fPn:fP
MD5:	94BA71EFD891C3DCB84D299A3569E0DA
SHA1:	D1377C913F96023629C1A07DB3BF23E0BB5F9005
SHA-256:	30F19B17612845ECB696342C4C9306B80FFCEC7BDC5ABA5DC83A9DA346270990
SHA-512:	E82A98D4BB3D4218A77A020B3DF08B6EBD14411C8345EDB9D152B31D3A85098764928DBFE1CA3831A8581FE1F32F15DB0341AD132CCB0AF58B3EDB234A7A594
Malicious:	**true**
Reputation:	low
Preview:	i.L...H

C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	
Process:	C:\Users\user\Desktop\OFFER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	610816
Entropy (8bit):	7.683539798870558
Encrypted:	false
SSDEEP:	12288:5pV+lmcosZeY2eCbJtTx31jbzNDWMEDBOzuZ2znyo3almjbbLSz9CUo:9cGVF9d1DNDWMYAzuIbyoqlMbPSzbo
MD5:	F0A3B70A92ECE3204289B3E1E25C9942
SHA1:	5AF0534294C9F5FD1ADA722919EC8583F88F2AC9
SHA-256:	0A09EC08C850081FFB281F5716859D62093A5F772266503CB67D5E49A4ECD4F4
SHA-512:	35E3E2924E5B0CA26CD8D25DD0AF84ED89196EF6B4C7202BA2E18EC1741C030CC7D53C86EF0FCC9A876DC151A38A5AB3979D9B948ADB8C2E1560D3FDD3501E0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 57%, Browse • Antivirus: Metadefender, Detection: 41%, Browse • Antivirus: ReversingLabs, Detection: 69%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....D.....>+.. ...@....@.. ....@.....*..O....@..xA..... ....H.....text...D.... ....`.rsrc...xA...@...B.....@..@.reloc.....P.....@..B..... +.....H.....e.....Y.....(....*&..(....*.s.....s.....s .....s!.....s".....*...0.....~....o#....+..*.0..... .....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0..<.....~.....((.....,!r...p.....()...o*...s+.....~.....+..*.0.....~.....+..*"......*.0..&.....(....r-..p~....o,...(-.....t.....+..*...0..&.....(....r9..p~....o,...(-.....

C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\OFFER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe:Zone.Identifier	
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.683539798870558
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:	OFFER.exe
File size:	610816
MD5:	f0a3b70a92ece3204289b3e1e25c9942
SHA1:	5af0534294c9f5fd1ada722919ec8583f88f2ac9
SHA256:	0a09ec08c850081ffb281f5716859d62093a5f772266503cb67d5e49a4ecd4f4
SHA512:	35e3e2924e5b0ca26cd8d25dd0af84ed89196ef6b4c7202ba2e18ec1741c030cc7d53c86ef0fcc9a876dc151a38a5ab3979d9b948adb8c2e1560d3fdd35011e0
SSDEEP:	12288:5pV+lmcosZeY2eCbJtTx31jbzNDWMEDBOzuZ2znyo3almjbbLSz9CUo:9cGVF9d1DNDWMYAzuIbyoqlMbPSzbo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....D.....>+... ...@....@.. .....@.....

File Icon

Icon Hash:	480f0f49194d4520

Static PE Info

General

Entrypoint:	0x492b3e
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:	0x5F990EE4 [Wed Oct 28 06:25:40 2020 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

General	
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x92aec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x94000	0x4178	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x90b44	0x90c00	False	0.811946783247	data	7.70065403732	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x4178	0x4200	False	0.340968276515	data	4.65497389104	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x94190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x945f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x956a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0x97c48	0x30	data		
RT_VERSION	0x97c78	0x314	data		
RT_MANIFEST	0x97f8c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

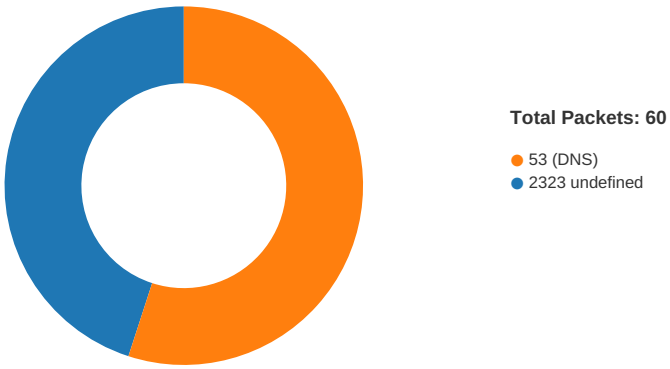
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	mQWh.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Controlador
ProductVersion	1.0.0.0
FileDescription	Controlador
OriginalFilename	mQWh.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 15:28:03.778383017 CET	49711	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:06.779992104 CET	49711	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:12.780513048 CET	49711	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:22.446753979 CET	49717	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:25.453433037 CET	49717	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:31.469504118 CET	49717	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:41.136913061 CET	49729	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:44.142489910 CET	49729	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:50.158615112 CET	49729	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:28:57.892918110 CET	49734	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:00.893838882 CET	49734	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:06.910063028 CET	49734	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:15.128210068 CET	49739	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:18.129841089 CET	49739	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:24.146588087 CET	49739	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:31.857831001 CET	49742	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:34.865459919 CET	49742	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:40.881633997 CET	49742	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:49.063406944 CET	49743	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:52.069961071 CET	49743	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:29:58.086153984 CET	49743	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:30:08.977169037 CET	49744	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:30:12.102895021 CET	49744	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:30:18.103403091 CET	49744	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:30:25.596973896 CET	49745	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:30:28.604291916 CET	49745	2323	192.168.2.3	37.18.96.19
Nov 24, 2020 15:30:34.620423079 CET	49745	2323	192.168.2.3	37.18.96.19

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 15:27:53.506155968 CET	55984	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:27:53.533616066 CET	53	55984	8.8.8.8	192.168.2.3
Nov 24, 2020 15:27:54.659101963 CET	64185	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:27:54.686460018 CET	53	64185	8.8.8.8	192.168.2.3
Nov 24, 2020 15:27:56.442240953 CET	65110	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:27:56.478300095 CET	53	65110	8.8.8.8	192.168.2.3
Nov 24, 2020 15:27:57.345671892 CET	58361	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:27:57.372770071 CET	53	58361	8.8.8.8	192.168.2.3
Nov 24, 2020 15:27:58.937705994 CET	63492	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:27:58.964807034 CET	53	63492	8.8.8.8	192.168.2.3
Nov 24, 2020 15:27:59.964009047 CET	60831	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:27:59.991353035 CET	53	60831	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:03.718260050 CET	60100	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:03.764199018 CET	53	60100	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:15.093889952 CET	53195	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:15.129780054 CET	53	53195	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:16.826072931 CET	50141	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:16.853127956 CET	53	50141	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:21.401735067 CET	53023	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:21.429003000 CET	53	53023	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:22.360163927 CET	49563	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:22.387494087 CET	53	49563	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:22.404793978 CET	51352	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:22.445501089 CET	53	51352	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:23.165205956 CET	59349	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:23.200990915 CET	53	59349	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:24.037941933 CET	57084	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:24.073755980 CET	53	57084	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:25.199189901 CET	58823	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:25.226290941 CET	53	58823	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:27.783973932 CET	57568	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 15:28:27.821347952 CET	53	57568	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:34.769733906 CET	50540	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:34.796920061 CET	53	50540	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:35.618417978 CET	54366	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:35.645675898 CET	53	54366	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:38.654897928 CET	53034	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:38.681972980 CET	53	53034	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:39.306180000 CET	57762	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:39.356237888 CET	53	57762	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:39.559573889 CET	55435	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:39.586956024 CET	53	55435	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:41.097023964 CET	50713	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:41.134298086 CET	53	50713	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:44.236629963 CET	56132	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:44.263674021 CET	53	56132	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:55.406728029 CET	58987	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:55.434057951 CET	53	58987	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:57.856010914 CET	56579	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:57.891792059 CET	53	56579	8.8.8.8	192.168.2.3
Nov 24, 2020 15:28:57.897439957 CET	60633	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:28:57.934497118 CET	53	60633	8.8.8.8	192.168.2.3
Nov 24, 2020 15:29:15.099493980 CET	61292	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:29:15.126679897 CET	53	61292	8.8.8.8	192.168.2.3
Nov 24, 2020 15:29:30.311285019 CET	63619	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:29:30.338418961 CET	53	63619	8.8.8.8	192.168.2.3
Nov 24, 2020 15:29:31.783803940 CET	64938	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:29:31.815838099 CET	61946	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:29:31.819479942 CET	53	64938	8.8.8.8	192.168.2.3
Nov 24, 2020 15:29:31.851372004 CET	53	61946	8.8.8.8	192.168.2.3
Nov 24, 2020 15:29:49.024101973 CET	64910	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:29:49.059978962 CET	53	64910	8.8.8.8	192.168.2.3
Nov 24, 2020 15:30:07.586671114 CET	52123	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:30:07.624885082 CET	53	52123	8.8.8.8	192.168.2.3
Nov 24, 2020 15:30:25.558933020 CET	56130	53	192.168.2.3	8.8.8.8
Nov 24, 2020 15:30:25.596074104 CET	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2020 15:28:03.718260050 CET	192.168.2.3	8.8.8.8	0x330b	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:28:22.404793978 CET	192.168.2.3	8.8.8.8	0x731b	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:28:41.097023964 CET	192.168.2.3	8.8.8.8	0xdf3e	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:28:57.856010914 CET	192.168.2.3	8.8.8.8	0x7759	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:29:15.099493980 CET	192.168.2.3	8.8.8.8	0xdf0b	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:29:31.815838099 CET	192.168.2.3	8.8.8.8	0xe3da	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:29:49.024101973 CET	192.168.2.3	8.8.8.8	0x8150	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:30:07.586671114 CET	192.168.2.3	8.8.8.8	0x371e	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 15:30:25.558933020 CET	192.168.2.3	8.8.8.8	0x748e	Standard query (0)	udochukwu.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

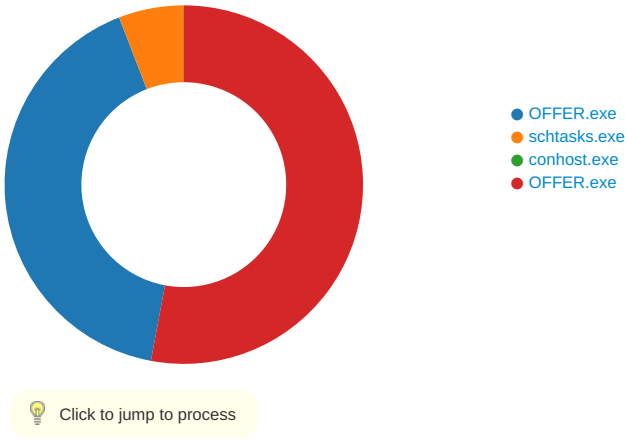
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 15:28:03.764199018 CET	8.8.8.8	192.168.2.3	0x330b	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:28:22.445501089 CET	8.8.8.8	192.168.2.3	0x731b	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 15:28:41.134298086 CET	8.8.8.8	192.168.2.3	0xdf3e	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:28:57.891792059 CET	8.8.8.8	192.168.2.3	0x7759	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:29:15.126679897 CET	8.8.8.8	192.168.2.3	0xdf0b	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:29:31.851372004 CET	8.8.8.8	192.168.2.3	0xe3da	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:29:49.059978962 CET	8.8.8.8	192.168.2.3	0x8150	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:30:07.624885082 CET	8.8.8.8	192.168.2.3	0x371e	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)
Nov 24, 2020 15:30:25.596074104 CET	8.8.8.8	192.168.2.3	0x748e	No error (0)	udochukwu.ddns.net		37.18.96.19	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: OFFER.exe PID: 6088 Parent PID: 5720

General

Start time:	15:27:58
Start date:	24/11/2020
Path:	C:\Users\user\Desktop\OFFER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OFFER.exe'
Imagebase:	0x720000
File size:	610816 bytes

MD5 hash:	F0A3B70A92ECE3204289B3E1E25C9942
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: 00000000.00000002.210666466.0000000002EA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.211065928.0000000003EA1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.211065928.0000000003EA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.211065928.0000000003EA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.210800137.0000000002F20000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	E9BD48	CopyFileW
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	E9BD48	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	55306D0	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\OFFER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp	success or wait	1	5530CA2	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e4 0e 99 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 0c 09 00 00 44 00 00 00 00 00 00 3e 2b 09 00 00 20 00 00 00 40 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P......D......>+... ...@.. ..@.. ....@................	success or wait	3	E9BD48	CopyFileW
C:\Users\user\AppData\Roaming\RplepwTnfZYE.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	E9BD48	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp	unknown	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	553095F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\OFFER.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	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,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 5436 Parent PID: 6088

General

Start time:	15:28:00
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RplepwTnfZYE' /XML 'C:\Users\user\AppData\Local\Temp\tmpB5D6.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp	unknown	2	success or wait	1	139AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB5D6.tmp	unknown	1646	success or wait	1	139ABD9	ReadFile

Analysis Process: conhost.exe PID: 4084 Parent PID: 5436

General

Start time:	15:28:00
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: OFFER.exe PID: 5056 Parent PID: 6088

General

Start time:	15:28:01
Start date:	24/11/2020
Path:	C:\Users\user\Desktop\OFFER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OFFER.exe
Imagebase:	0xf90000
File size:	610816 bytes
MD5 hash:	F0A3B70A92ECE3204289B3E1E25C9942
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	58507A1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	585089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	58507A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	58507A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\OFFER.exe:Zone.Identifier	success or wait	1	5850B41	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	69 d9 4c 96 d0 90 d8 48	i.L....H	success or wait	1	5850A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\OFFER.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\OFFER.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5850A53	ReadFile

Disassembly

Code Analysis