ID: 629870
Sample Name:
692BB93169319EBA2F556174D781A8636D610A67E6838.exe
Cookbook: default.jbs
Time: 05:18:10
Date: 19/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 692BB93169319EBA2F556174D781A8636D610A67E6838.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
AV Detection 6
E-Banking Fraud 6
Data Obfuscation 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Boot Survival 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
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 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
World Map of Contacted IPs 11
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log 13
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 14
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ople.exe.vbs 14
C:\Users\user\AppData\Roaming\etwa\ople.exe.exe 14
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 17
Sections 17
Resources 18
Imports 18
Version Infos 18
Possible Origin 18

Network Behavior 19
TCP Packets 19
UDP Packets 20
DNS Queries 20
DNS Answers 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: 692BB93169319EBA2F556174D781A8636D610A67E6838.exePID: 5844, Parent PID: 2092 21
General 21
File Activities 22
Analysis Process: conhost.exePID: 6076, Parent PID: 5844 22
General 22
Analysis Process: RegAsm.exePID: 5596, Parent PID: 5844 22
General 22
File Activities 23
File Created 23
File Written 23
File Read 23
Analysis Process: wscript.exePID: 2208, Parent PID: 3616 24
General 24
File Activities 24
Analysis Process: ople.exe.exePID: 1796, Parent PID: 2208 24
General 24
File Activities 25
File Read 25
Analysis Process: conhost.exePID: 1720, Parent PID: 1796 25
General 25
Analysis Process: RegAsm.exePID: 1428, Parent PID: 1796 25
General 25
File Activities 26
File Created 26
File Written 26
File Read 27
Disassembly 27

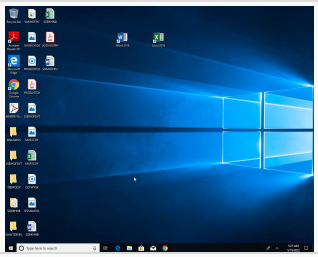
Windows Analysis Report

692BB93169319EBA2F556174D781A8636D610A67E6838.exe

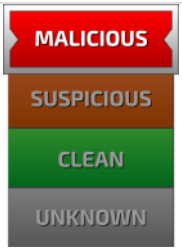
Overview

General Information

Sample Name:	692BB93169319EBA2F556174D781A8636D610A67E6838.exe
Analysis ID:	629870
MD5:	a93162e62b49a5.
SHA1:	b0c48a0fc41897…
SHA256:	692bb93169319e.
Tags:	exe NanoCore RAT
Infos:	



Detection



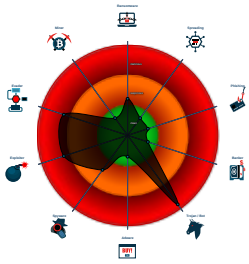
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- 692BB93169319EBA2F556174D781A8636D610A67E6838.exe (PID: 5844 cmdline: "C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe" MD5: A93162E62B49A591E0D481E030FFC9EA)
  - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 5596 cmdline: "C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe" MD5: 6FD7592411112729BF6B1F2F6C34899F)
- wscript.exe (PID: 2208 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ople.exe.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - ople.exe.exe (PID: 1796 cmdline: C:\Users\user\AppData\Roaming\etwa\ople.exe.exe MD5: CA51A0A9E3EF192B26D9818DC4EC5FF0)
    - conhost.exe (PID: 1720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - RegAsm.exe (PID: 1428 cmdline: C:\Users\user\AppData\Roaming\etwa\ople.exe.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "3b5167aa-3858-4f80-81dc-688e9982",
  "Group": "AtikuVSDino",
  "Domain1": "dinolachy.duckdns.org",
  "Domain2": "127.0.0.1",
  "Port": 5626,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.296930304.0000000000402000.00000040.80000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000000.296930304.0000000000402000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000000.296930304.0000000000402000.00000040.80000000.00040000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000003.00000002.513573670.00000000056A0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000003.00000002.513573670.00000000056A0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost

Click to see the 43 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.RegAsm.exe.56a4629.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
3.2.RegAsm.exe.56a4629.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
3.2.RegAsm.exe.56a4629.7.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.2.RegAsm.exe.56a4629.7.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xb14f:$x2: NanoCore.ClientPlugin • 0xb184:$x3: NanoCore.ClientPluginHost • 0xb143:$i2: IClientData • 0xb165:$i3: IClientNetwork • 0xb174:$i5: IClientDataHost • 0xb19e:$i6: IClientLoggingHost • 0xb1b1:$i7: IClientNetworkHost • 0xb1c4:$i8: IClientUIHost • 0xb1d2:$i9: IClientNameObjectCollection • 0xb1ee:$i10: IClientReadOnlyNameObjectCollection • 0xaf41:$s1: ClientPlugin • 0xb158:$s1: ClientPlugin • 0x10179:$s6: get_ClientSettings
12.2.RegAsm.exe.2ffb670.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 88 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Data Obfuscation

Sigma detected: Drops script at startup location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

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

Drops VBS files to the startup folder

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

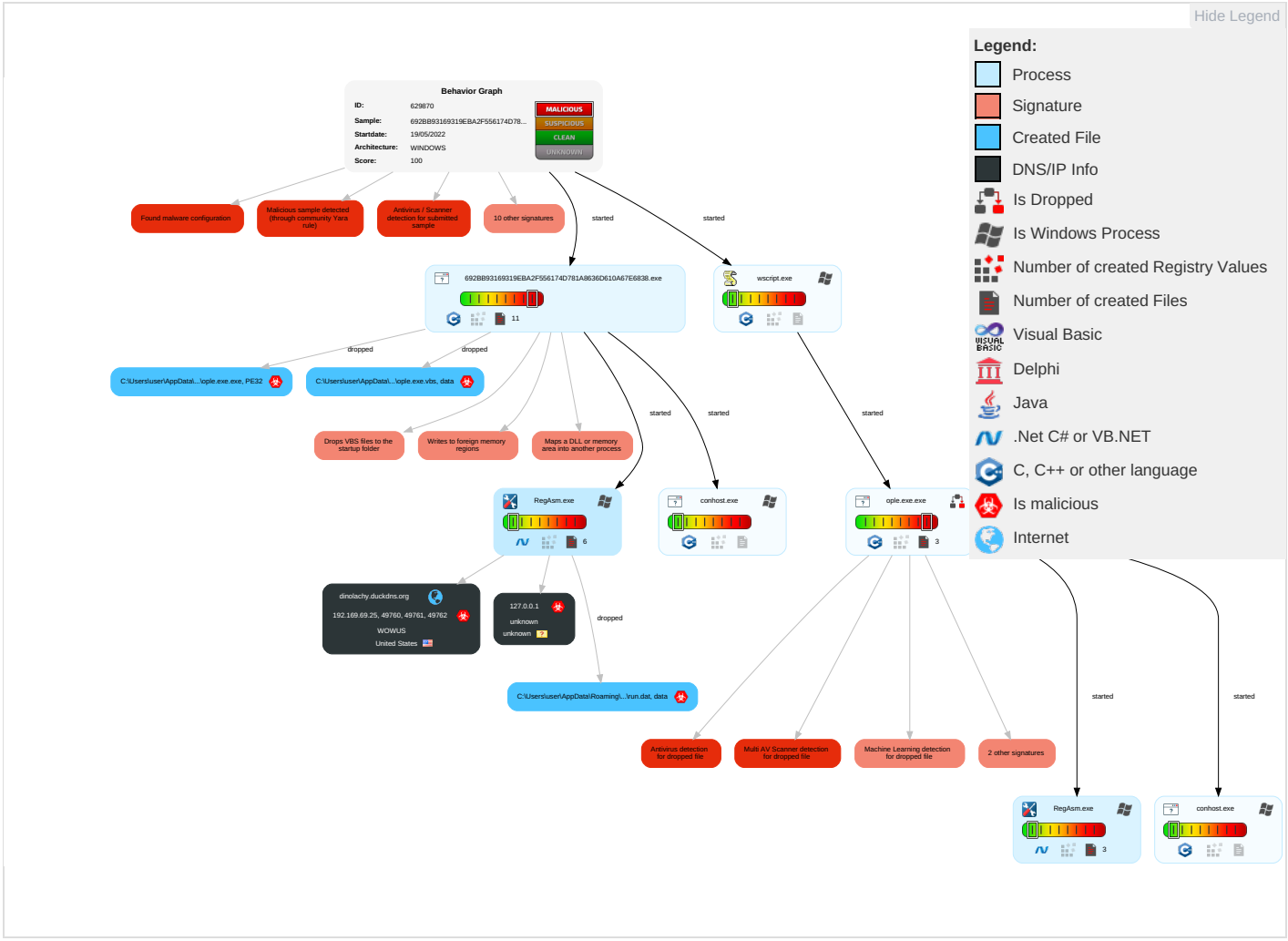
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 1 Scripting	2 Registry Run Keys / Startup Folder	2 1 2 Process Injection	1 1 Masquerading	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	2 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Scripting	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	2 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
692BB93169319EBA2F556174D781A8636D610A67E6838.exe	72%	Virustotal		Browse
692BB93169319EBA2F556174D781A8636D610A67E6838.exe	41%	Metadefender		Browse
692BB93169319EBA2F556174D781A8636D610A67E6838.exe	73%	ReversingLabs	Win32.Trojan.AgentTesla	
692BB93169319EBA2F556174D781A8636D610A67E6838.exe	100%	Avira	HEUR/AGEN.1213119	
692BB93169319EBA2F556174D781A8636D610A67E6838.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\etwa\ople.exe.exe	100%	Avira	HEUR/AGEN.1213119	
C:\Users\user\AppData\Roaming\etwa\ople.exe.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\etwa\ople.exe.exe	63%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.692BB93169319EBA2F556174D781A8636D610A67E6838.exe.260000.0.unpack	100%	Avira	HEUR/AGEN.1213119		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.ople.exe.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1213119		Download File
3.2.RegAsm.exe.56a0000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.0.692BB93169319EBA2F556174D781A8636D610A67E6838.exe.260000.0.unpack	100%	Avira	HEUR/AGEN.1213119		Download File
7.2.ople.exe.exe.ab0000.0.unpack	100%	Avira	HEUR/AGEN.1213119		Download File
12.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
dinolachy.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	1%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	
dinolachy.duckdns.org	1%	Virustotal		Browse
dinolachy.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

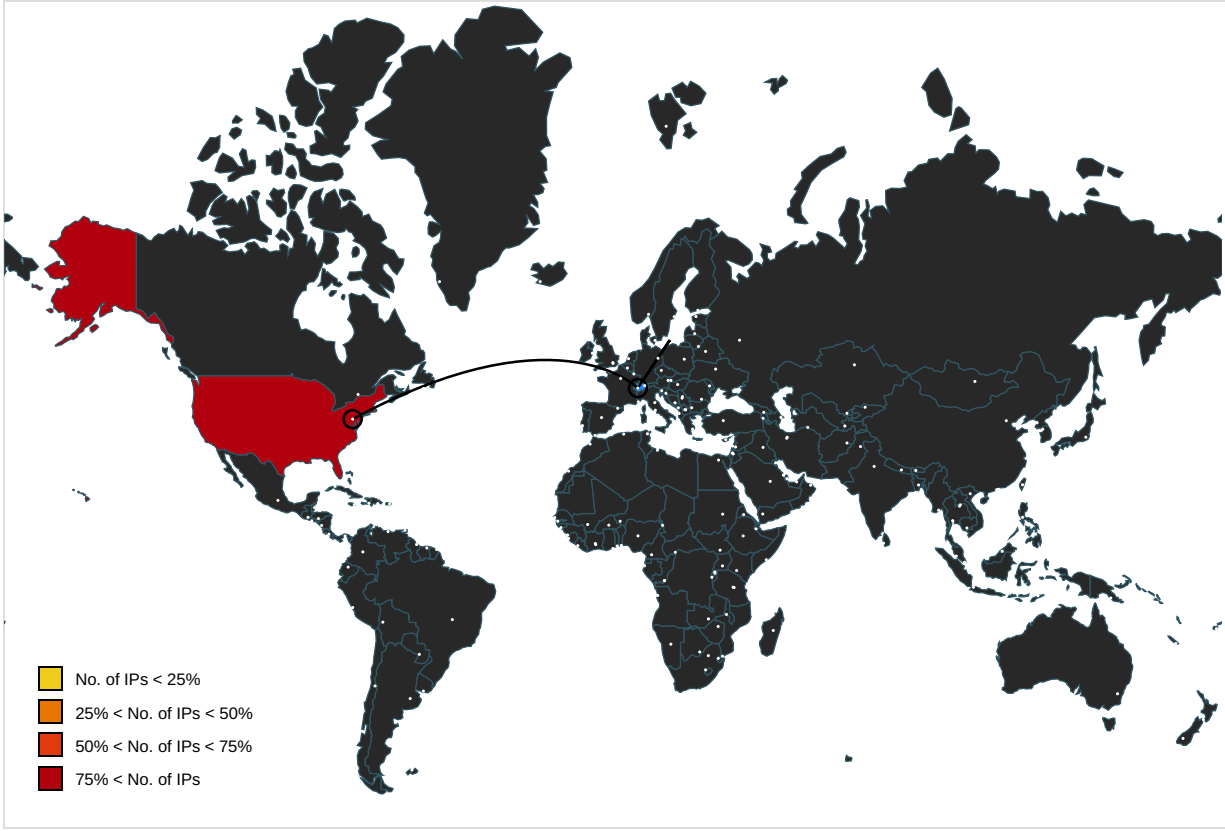
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dinolachy.duckdns.org	192.169.69.25	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
dinolachy.duckdns.org	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.169.69.25	dinolachy.duckdns.org	United States		23033	WOWUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	629870
Start date and time: 19/05/202205:18:10	2022-05-19 05:18:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	692BB93169319EBA2F556174D781A8636D610A67E6838.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:	30
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.expl.evad.winEXE@10/4@12/2

EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 87.3% (good quality ratio 79.3%) • Quality average: 77.4% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target RegAsm.exe, PID 1428 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:19:25	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ople.exe.vbs
05:19:40	API Interceptor	1x Sleep call for process: ople.exe.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:LI:LI
MD5:	B0D520A58AFBB2268CEB35E278A4EB33
SHA1:	15B41F5F9DC6456482F03330B5450F3C0784F9A3
SHA-256:	D9BE84474B3876A55B0D1BD3971001A9F50C7F3039CEE9C09209C74E9C2BD316
SHA-512:	7E91CC1295EA5B68E151795ED5D6EC93105546405C02C56DC4A459A47865610D164D40635A0E01F91C4B4F63C353BEA0E7947DD4236BD189231235D0B66C605
Malicious:	**true**
Reputation:	low
Preview:	f..dF9.H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ople.exe.vbs

Process:	C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe
File Type:	data
Category:	dropped
Size (bytes):	304
Entropy (8bit):	3.410548573208775
Encrypted:	false
SSDEEP:	6:xPW+YR4lAINl1fYlfm3OOQd4l1RIlRKUEZgIJPZ60mlRA6DA6nMWl1fYlxCv:xQ4lAN0+vcIlRKMJelRRFSji
MD5:	36615C3E591704897CAC5551FFD58553
SHA1:	ABDC43118D030E3716FA302B5E6B5AA6D7FD3C72
SHA-256:	CF648418AC15FCD4CD81C2AD4E289F149B52FCA8A6198F39EFBE52D71C602B04
SHA-512:	ACE72BF54585FD266CCD8732146C8D1BCE5E4731EC44C18A005759622C938D34C435BED0EAC1EEECCAC732EC1C125566862748B101383BAE8D2C16B45525F D7
Malicious:	**true**
Reputation:	low
Preview:	O.n. .E.r.r.o.r. .R.e.s.u.m.e. .N.e.x.t...S.e.t. .S.h.e.l.l.V.a.r. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(."W.S.c.r.i.p.t...S.h.e.l.l.").)...S.h.e.l.l.V.a.r...E.x.e.c.("C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.e.t.w.a.\.o.p.l.e...e.x.e...e.x.e.").)...S.e.t.S.h.e.l.l.V.a.r. .=.N.o.t.h.i.n.g.

C:\Users\user\AppData\Roaming\etwa\ople.exe.exe

Process:	C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	409170
Entropy (8bit):	7.3076840802364
Encrypted:	false
SSDEEP:	6144:PuWieVAGW6qGWdFlnHCDFrNAiX1AS0mrSMnBX21Cjna06R8fpR4Qq3fS:PVl+nHAZ19RrSMdd6qFyS
MD5:	CA51A0A9E3EF192B26D9818DC4EC5FF0
SHA1:	7D56B8436D501E6CDA892E61FA29BEEEDF65DA0E

SHA-256:	D0250A0B19CC73D8E6A4C97EA7935BA06BA70DD1FB9EEA8C44AEA396DD792A6E
SHA-512:	1997CFD7D25FFE7BB59A9C8A6F7E009D4B693FF4019B0E6698CEFE9FEBD393848C5F4DE9DD3025354E4059EAAD0B29CE2D3B141ED4586B1C7C8DB763035828 15
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f.....8h.....8h.....8h.....!.....!.....!.....8h.....9.....9.....9. .....Rich.....PE..L.....]..... ".....@.....@.....!.....`.....8...P.....p...@..... .....text...G..... ..`.rdata..(Z.....\.....@..@.data.....0..... .....@....gfids.....P.....(.....@..@.rsrc.....`.....*.....@..@.re loc..8.....@..B.....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.307692888739697
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	692BB93169319EBA2F556174D781A8636D610A67E6838.exe
File size:	409169
MD5:	a93162e62b49a591e0d481e030ffc9ea
SHA1:	b0c48a0fc418977051bea837c16aa7928f654da7
SHA256:	692bb93169319eba2f556174d781a8636d610a67e6838e19300a8a2454cd8b2b
SHA512:	2f5c74acd25c9a7fae88736e25e526155d09d5c1c0f66c833c8e6e0c3dfd74fd7d53438089d5de5a07fd2935a78a27a13d3d6ddeef020d42ecafb38497926c25
SSDEEP:	6144:PuWieVAGW6qGWdFlnHCDFrNAiX1AS0mrSMnBX21Cjna06R8fpR4Qq3fm:PVl+nHAZ19RrSMdd6qFym
TLSH:	E3949D52F29698A5E426B1F8A8359D32122B7D9558348A0B31BB312D4E733D3DC77E0F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f.....8h.....8h.....8h.....!.....!.....!.....8h.....9.....9.....9.....Rich.....

File Icon

Icon Hash:	4552445c54463289

Static PE Info

General

Entrypoint:	0x402212
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5DDBF1DC [Mon Nov 25 15:23:08 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	695a88385098872b689faf1f231ef8ea

Entrypoint Preview

Instruction
call 00007FBE38700972h
jmp 00007FBE3870058Dh
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007FBE3870071Bh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007FBE3870070Ch
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007FBE3870070Eh
add edx, 28h
cmp edx, esi
jne 00007FBE387006ECh
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007FBE387006FBh
call 00007FBE38700E4Fh
test eax, eax
jne 00007FBE38700705h
xor al, al
ret
mov eax, dword ptr fs:[00000018h]
push esi
mov esi, 00413794h
mov edx, dword ptr [eax+04h]
jmp 00007FBE38700706h
cmp edx, eax
je 00007FBE38700712h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007FBE387006F2h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007FBE38700709h

Instruction
mov byte ptr [004137B0h], 00000001h
call 00007FBE38700C66h
call 00007FBE387010ECh
test al, al
jne 00007FBE38700706h
xor al, al
pop ebp
ret
call 00007FBE38702A00h
test al, al
jne 00007FBE3870070Ch
push 00000000h
call 00007FBE387010FDh
pop ecx
jmp 00007FBE387006EBh
mov al, 01h
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 0Ch
push esi
mov esi, dword ptr [ebp+08h]
test esi, esi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x12114	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x18b90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2f000	0xe38	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11a50	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x11a70	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0x1b8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xbf47	0xc000	False	0.579060872396	data	6.64391063708	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x5a28	0x5c00	False	0.417246942935	data	4.87173398485	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x13000	0x11b8	0x800	False	0.17236328125	DOS executable (block device driver \277DN)	2.05377921789	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x15000	0xac	0x200	False	0.271484375	data	1.40558316368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x18b90	0x18c00	False	0.210611979167	data	4.88160389879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x2f000	0xe38	0x1000	False	0.744140625	data	6.17873004973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x164b8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x16920	0x10a8	data	English	United States
RT_ICON	0x179c8	0x25a8	data	English	United States
RT_ICON	0x19f70	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x1e198	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 33554431, next used block 33554431	English	United States
RT_GROUP_ICON	0x2e9c0	0x4c	data	English	United States
RT_VERSION	0x161f0	0x2c8	data	English	United States
RT_MANIFEST	0x2ea10	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	VirtualProtect, GetConsoleWindow, CreateFileW, DecodePointer, WriteConsoleW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, HeapReAlloc, HeapSize, GetProcessHeap, GetStringTypeW, GetFileType, SetStdHandle, LCMapStringW, CompareStringW, SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCPInfo, GetOEMCP, IsValidCodePage, FindNextFileA, FindFirstFileExA, FindClose, CloseHandle, HeapAlloc, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, GetCurrentProcess, TerminateProcess, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameA, MultiByteToWideChar, WideCharToMultiByte, ExitProcess, GetModuleHandleExW, GetCommandLineA, GetCommandLineW, GetACP, HeapFree, RaiseException
imagehlp.dll	UnDecorateSymbolName, SymGetSymFromAddr64
MAPI32.dll	
USER32.dll	GetAncestor, SetWindowPos, ChangeMenuA, BroadcastSystemMessage, SubtractRect, IsDialogMessageA, CountClipboardFormats
mscms.dll	DeleteColorTransform, InstallColorProfileA, SetColorProfileHeader, GetPS2ColorRenderingIntent, SetColorProfileElementReference
WINSPOOL.DRV	EnumPrinterDataW, OpenPrinterA, EnumPrinterKeyA
ODBC32.dll	
msi.dll	

Version Infos

Description	Data
LegalCopyright	Copyright (C) land-born 2019
InternalName	cardsharper.exe
FileVersion	8.2.1.4
CompanyName	vanes
ProductName	aggeration
ProductVersion	7.6.0.2
FileDescription	spermary
OriginalFilename	unobservant.exe
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 05:19:35.391271114 CEST	49760	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:35.604505062 CEST	5626	49760	192.169.69.25	192.168.2.4
May 19, 2022 05:19:35.604670048 CEST	49760	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:35.661648035 CEST	49760	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:35.899727106 CEST	5626	49760	192.169.69.25	192.168.2.4
May 19, 2022 05:19:40.045200109 CEST	49761	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:40.334722042 CEST	5626	49761	192.169.69.25	192.168.2.4
May 19, 2022 05:19:40.334908962 CEST	49761	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:40.355438948 CEST	49761	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:40.629517078 CEST	5626	49761	192.169.69.25	192.168.2.4
May 19, 2022 05:19:44.675549030 CEST	49762	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:44.999265909 CEST	5626	49762	192.169.69.25	192.168.2.4
May 19, 2022 05:19:44.999759912 CEST	49762	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:45.004966021 CEST	49762	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:19:45.291423082 CEST	5626	49762	192.169.69.25	192.168.2.4
May 19, 2022 05:20:04.840961933 CEST	49774	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:05.154113054 CEST	5626	49774	192.169.69.25	192.168.2.4
May 19, 2022 05:20:05.154316902 CEST	49774	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:05.161387920 CEST	49774	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:05.464230061 CEST	5626	49774	192.169.69.25	192.168.2.4
May 19, 2022 05:20:09.601588964 CEST	49775	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:09.902873039 CEST	5626	49775	192.169.69.25	192.168.2.4
May 19, 2022 05:20:09.903219938 CEST	49775	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:09.904114008 CEST	49775	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:10.191227913 CEST	5626	49775	192.169.69.25	192.168.2.4
May 19, 2022 05:20:14.236185074 CEST	49776	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:14.530116081 CEST	5626	49776	192.169.69.25	192.168.2.4
May 19, 2022 05:20:14.530278921 CEST	49776	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:14.530742884 CEST	49776	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:14.815737009 CEST	5626	49776	192.169.69.25	192.168.2.4
May 19, 2022 05:20:34.964564085 CEST	49829	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:35.244076967 CEST	5626	49829	192.169.69.25	192.168.2.4
May 19, 2022 05:20:35.244360924 CEST	49829	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:35.251326084 CEST	49829	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:35.520592928 CEST	5626	49829	192.169.69.25	192.168.2.4
May 19, 2022 05:20:39.559667110 CEST	49837	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:39.872410059 CEST	5626	49837	192.169.69.25	192.168.2.4
May 19, 2022 05:20:39.872554064 CEST	49837	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:39.873094082 CEST	49837	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:40.164750099 CEST	5626	49837	192.169.69.25	192.168.2.4
May 19, 2022 05:20:44.291788101 CEST	49839	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:44.577816963 CEST	5626	49839	192.169.69.25	192.168.2.4
May 19, 2022 05:20:44.579777002 CEST	49839	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:44.602205038 CEST	49839	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:20:44.877954006 CEST	5626	49839	192.169.69.25	192.168.2.4
May 19, 2022 05:21:04.218692064 CEST	49866	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:04.455672026 CEST	5626	49866	192.169.69.25	192.168.2.4
May 19, 2022 05:21:04.455786943 CEST	49866	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:04.458276033 CEST	49866	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:04.747319937 CEST	5626	49866	192.169.69.25	192.168.2.4
May 19, 2022 05:21:08.868937969 CEST	49869	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:09.173266888 CEST	5626	49869	192.169.69.25	192.168.2.4
May 19, 2022 05:21:09.173451900 CEST	49869	5626	192.168.2.4	192.169.69.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 05:21:09.174114943 CEST	49869	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:09.475833893 CEST	5626	49869	192.169.69.25	192.168.2.4
May 19, 2022 05:21:13.529231071 CEST	49871	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:13.753601074 CEST	5626	49871	192.169.69.25	192.168.2.4
May 19, 2022 05:21:13.753717899 CEST	49871	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:13.763097048 CEST	49871	5626	192.168.2.4	192.169.69.25
May 19, 2022 05:21:14.037683010 CEST	5626	49871	192.169.69.25	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2022 05:19:35.271678925 CEST	60506	53	192.168.2.4	8.8.8.8
May 19, 2022 05:19:35.380067110 CEST	53	60506	8.8.8.8	192.168.2.4
May 19, 2022 05:19:39.935419083 CEST	64277	53	192.168.2.4	8.8.8.8
May 19, 2022 05:19:40.044132948 CEST	53	64277	8.8.8.8	192.168.2.4
May 19, 2022 05:19:44.650464058 CEST	56076	53	192.168.2.4	8.8.8.8
May 19, 2022 05:19:44.667726994 CEST	53	56076	8.8.8.8	192.168.2.4
May 19, 2022 05:20:04.727262020 CEST	60381	53	192.168.2.4	8.8.8.8
May 19, 2022 05:20:04.837091923 CEST	53	60381	8.8.8.8	192.168.2.4
May 19, 2022 05:20:09.485280991 CEST	56509	53	192.168.2.4	8.8.8.8
May 19, 2022 05:20:09.593802929 CEST	53	56509	8.8.8.8	192.168.2.4
May 19, 2022 05:20:14.216454983 CEST	54069	53	192.168.2.4	8.8.8.8
May 19, 2022 05:20:14.234416008 CEST	53	54069	8.8.8.8	192.168.2.4
May 19, 2022 05:20:34.752480030 CEST	61497	53	192.168.2.4	8.8.8.8
May 19, 2022 05:20:34.861716032 CEST	53	61497	8.8.8.8	192.168.2.4
May 19, 2022 05:20:39.538358927 CEST	60418	53	192.168.2.4	8.8.8.8
May 19, 2022 05:20:39.558176041 CEST	53	60418	8.8.8.8	192.168.2.4
May 19, 2022 05:20:44.182333946 CEST	64259	53	192.168.2.4	8.8.8.8
May 19, 2022 05:20:44.290632010 CEST	53	64259	8.8.8.8	192.168.2.4
May 19, 2022 05:21:04.108495951 CEST	58715	53	192.168.2.4	8.8.8.8
May 19, 2022 05:21:04.217644930 CEST	53	58715	8.8.8.8	192.168.2.4
May 19, 2022 05:21:08.758953094 CEST	57816	53	192.168.2.4	8.8.8.8
May 19, 2022 05:21:08.867835999 CEST	53	57816	8.8.8.8	192.168.2.4
May 19, 2022 05:21:13.507783890 CEST	53916	53	192.168.2.4	8.8.8.8
May 19, 2022 05:21:13.527236938 CEST	53	53916	8.8.8.8	192.168.2.4

DNS Queries

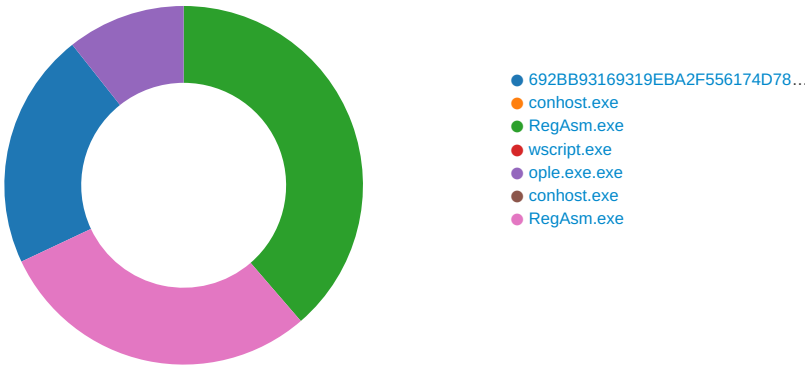
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 19, 2022 05:19:35.271678925 CEST	192.168.2.4	8.8.8.8	0x19ec	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:19:39.935419083 CEST	192.168.2.4	8.8.8.8	0x5d07	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:19:44.650464058 CEST	192.168.2.4	8.8.8.8	0x6fcf	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:20:04.727262020 CEST	192.168.2.4	8.8.8.8	0xf60b	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:20:09.485280991 CEST	192.168.2.4	8.8.8.8	0x474	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:20:14.216454983 CEST	192.168.2.4	8.8.8.8	0x37a	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:20:34.752480030 CEST	192.168.2.4	8.8.8.8	0xd39f	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:20:39.538358927 CEST	192.168.2.4	8.8.8.8	0x6194	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:20:44.182333946 CEST	192.168.2.4	8.8.8.8	0x4b2c	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:21:04.108495951 CEST	192.168.2.4	8.8.8.8	0x30ea	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:21:08.758953094 CEST	192.168.2.4	8.8.8.8	0xa247	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)
May 19, 2022 05:21:13.507783890 CEST	192.168.2.4	8.8.8.8	0x5cde	Standard query (0)	dinolachy.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 19, 2022 05:19:35.380067110 CEST	8.8.8.8	192.168.2.4	0x19ec	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:19:40.044132948 CEST	8.8.8.8	192.168.2.4	0x5d07	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:19:44.667726994 CEST	8.8.8.8	192.168.2.4	0x6fcf	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:20:04.837091923 CEST	8.8.8.8	192.168.2.4	0xf60b	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:20:09.593802929 CEST	8.8.8.8	192.168.2.4	0x474	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:20:14.234416008 CEST	8.8.8.8	192.168.2.4	0x37a	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:20:34.861716032 CEST	8.8.8.8	192.168.2.4	0xd39f	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:20:39.558176041 CEST	8.8.8.8	192.168.2.4	0x6194	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:20:44.290632010 CEST	8.8.8.8	192.168.2.4	0x4b2c	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:21:04.217644930 CEST	8.8.8.8	192.168.2.4	0x30ea	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:21:08.867835999 CEST	8.8.8.8	192.168.2.4	0xa247	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)
May 19, 2022 05:21:13.527236938 CEST	8.8.8.8	192.168.2.4	0x5cde	No error (0)	dinolachy.duckdns.org		192.169.69.25	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: 692BB93169319EBA2F556174D781A8636D610A67E6838.exe PID: 5844, Parent PID: 2092

General

Target ID:	0
Start time:	05:19:17
Start date:	19/05/2022
Path:	C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe"
Imagebase:	0x260000

File size:	409169 bytes
MD5 hash:	A93162E62B49A591E0D481E030FFC9EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.269192497.0000000000D80000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.269192497.0000000000D80000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.269192497.0000000000D80000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.269192497.0000000000D80000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.269192497.0000000000D80000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Analysis Process: conhost.exe PID: **6076**, Parent PID: **5844**

General

Target ID:	1
Start time:	05:19:18
Start date:	19/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: RegAsm.exe PID: **5596**, Parent PID: **5844**

General

Target ID:	3
Start time:	05:19:25
Start date:	19/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\692BB93169319EBA2F556174D781A8636D610A67E6838.exe"
Imagebase:	0xa90000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.513573670.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.513573670.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.513573670.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.513573670.00000000056A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.509119262.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.509119262.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.509119262.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.266056234.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.266056234.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.266056234.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.510200651.0000000002D91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.513552281.0000000005650000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.513552281.0000000005650000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.513552281.0000000005650000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.511424469.0000000003DD9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.511424469.0000000003DD9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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	6D49CF06	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	6D49CF06	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	6C2EBEFF	CreateDirectoryW
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	6C2E1E60	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	6C2EBEFF	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	6C2EBEFF	CreateDirectoryW

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	0	8	66 fd 04 64 46 39 fd 48	fdF9H	success or wait	1	6C2E1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D47CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D47CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D47CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6D3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	4096	success or wait	1	6D45D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	unknown	512	success or wait	1	6D45D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D475705	unknown

Analysis Process: wscript.exe PID: **2208**, Parent PID: **3616**

General

Target ID:	6
Start time:	05:19:35
Start date:	19/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ople.exe.vbs"
Imagebase:	0x7ff784990000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ople.exe.exe PID: **1796**, Parent PID: **2208**

General

Target ID:	7
Start time:	05:19:36
Start date:	19/05/2022
Path:	C:\Users\user\AppData\Roaming\etwa\ople.exe.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\etwa\ople.exe.exe
Imagebase:	0xab0000
File size:	409170 bytes
MD5 hash:	CA51A0A9E3EF192B26D9818DC4EC5FF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.301093367.0000000002A00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.301093367.0000000002A00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.301093367.0000000002A00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.301093367.0000000002A00000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.301093367.0000000002A00000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 63%, ReversingLabs
Reputation:	low

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\Roaming\etwa\ople.exe.exe	0	409170	success or wait	1	2A4003D	NtReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	10D3471	ReadFile

Analysis Process: conhost.exe PID: **1720**, Parent PID: **1796**

General

Target ID:	8
Start time:	05:19:36
Start date:	19/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: RegAsm.exe PID: **1428**, Parent PID: **1796**

General

Target ID:	12
Start time:	05:19:40
Start date:	19/05/2022

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\etwa\ople.exe.exe
Imagebase:	0xca0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.296930304.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.296930304.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.296930304.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.319192237.0000000003F99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.319192237.0000000003F99000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.318213068.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.318213068.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.318213068.0000000000402000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.318967216.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.318967216.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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	6D49CF06	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	6D49CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D7AC78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D7AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D47CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D47CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D47CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C2E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C2E1B4F	ReadFile

Disassembly

No disassembly