ID: 435328
Sample Name: wmaJOYGy7Q
Cookbook: default.jbs
Time: 12:27:50
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

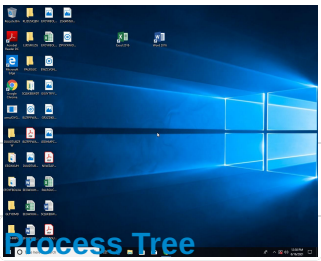
Windows Analysis Report wmaJOYGy7Q

Overview

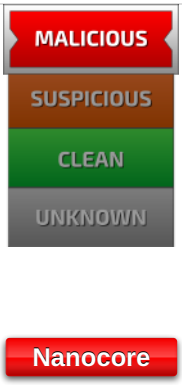
General Information

Sample Name:	wmaJOYGy7Q (renamed file extension from none to exe)
Analysis ID:	435328
MD5:	5688c69c437984..
SHA1:	09a30ec730d1fdf..
SHA256:	62801897ae3411..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

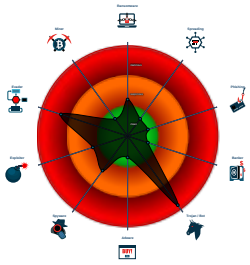


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



- **System is w10x64**
- wmaJOYGy7Q.exe (PID: 5344 cmdline: 'C:\Users\user\Desktop\wmaJOYGy7Q.exe' MD5: 5688C69C4379841EEE42DCAEC2DBF55A)
  - RegAsm.exe (PID: 4764 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - schtasks.exe (PID: 5812 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8A08.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegAsm.exe (PID: 6140 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "18773cd6-e296-4327-b004-0088e2e8",
  "Group": "WEALTH",
  "Domain1": "185.140.53.154",
  "Domain2": "wealthybillionaire.ddns.net",
  "Port": 5540,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.481468397.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.481468397.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.481468397.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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

Source	Rule	Description	Author	Strings
00000001.00000002.263955446.000000000365 8000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4347f:$x1: NanoCore.ClientPluginHost • 0x7615f:$x1: NanoCore.ClientPluginHost • 0xa8e2f:$x1: NanoCore.ClientPluginHost • 0x434bc:$x2: IClientNetworkHost • 0x7619c:$x2: IClientNetworkHost • 0xa8e6c:$x2: IClientNetworkHost • 0x46fef:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x79ccf:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xac99f:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.263955446.000000000365 8000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegAsm.exe.39c063c.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x287a1:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287ce:$x2: IClientNetworkHost
5.2.RegAsm.exe.39c063c.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x287a1:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2987c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x287bb:$s5: IClientLoggingHost
5.2.RegAsm.exe.39c063c.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
5.2.RegAsm.exe.299caf0.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
5.2.RegAsm.exe.299caf0.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 68 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- 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)
- .NET source code contains very large array initializations

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)

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

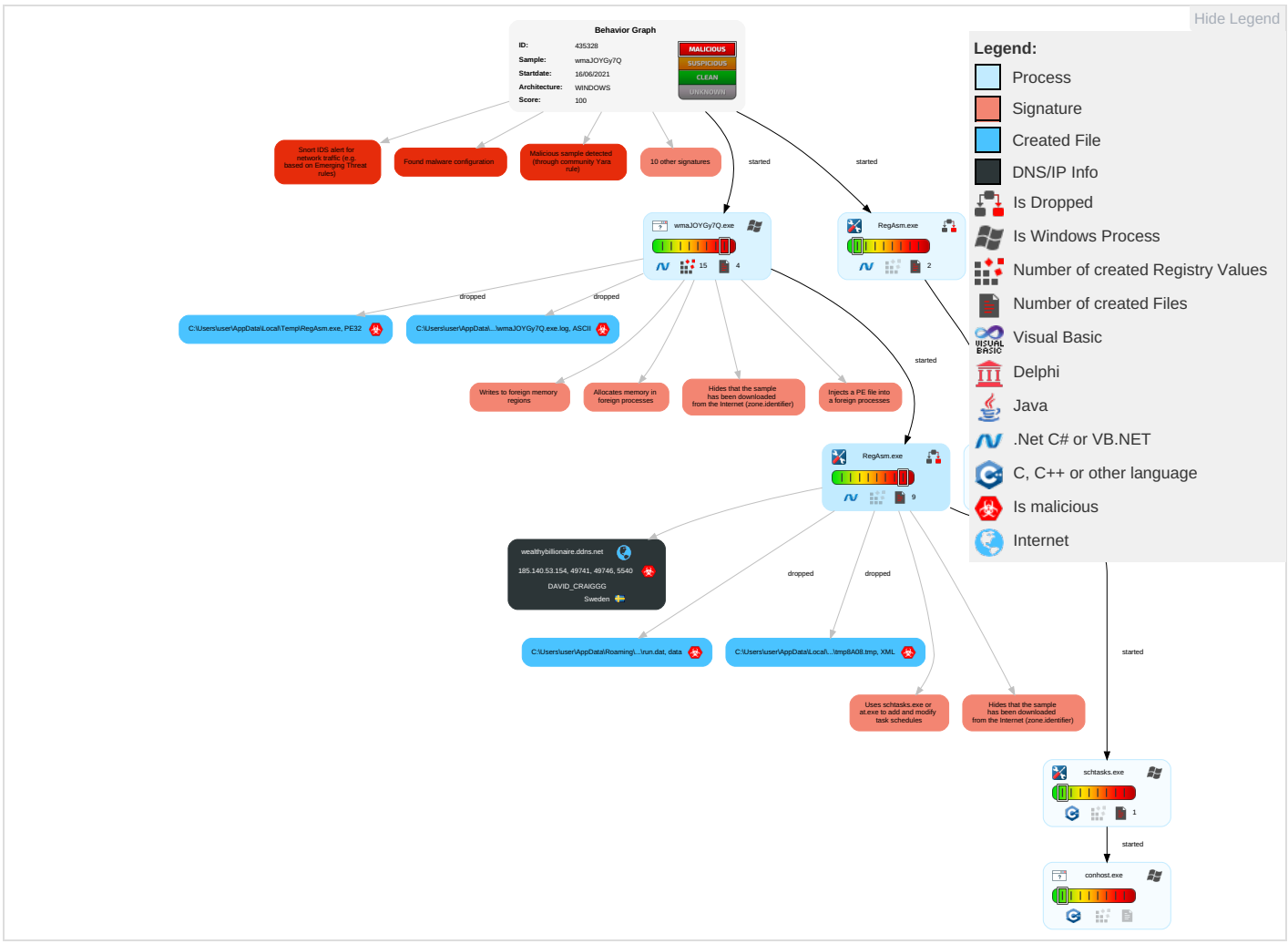
Remote Access Functionality:

- 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	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1	Input Capture 2 1	Security Software Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

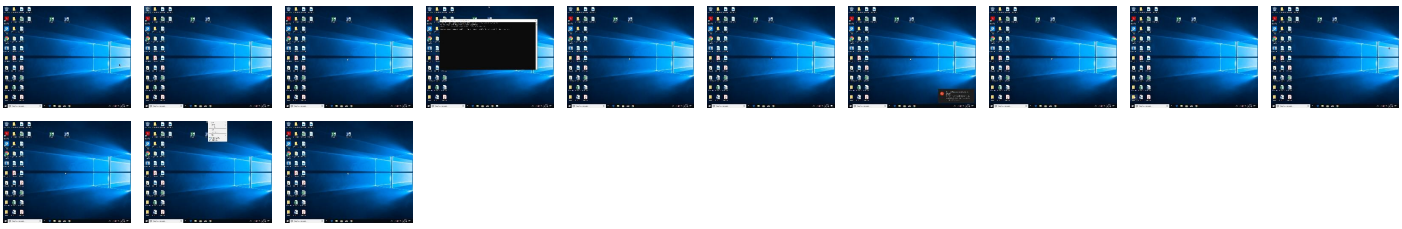
Behavior Graph



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
wmaJOYGy7Q.exe	30%	Virustotal		Browse
wmaJOYGy7Q.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	
wmaJOYGy7Q.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegAsm.exe.5250000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.pki.goog/gsr1/gsr1.crl0;	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g%%_	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	Avira URL Cloud	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
185.140.53.154	0%	Avira URL Cloud	safe	
wealthybillionaire.ddns.net	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/zdATt0Ex_Fk.crl0	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://pki.goog/repo/certs/gts1c3.der0	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthybillionaire.ddns.net	185.140.53.154	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.140.53.154	true	• Avira URL Cloud: safe	unknown
wealthybillionaire.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.154	wealthybillionaire.ddns.net	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435328
Start date:	16.06.2021
Start time:	12:27:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wmaJOYGy7Q (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	31
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@8/8@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.8% (good quality ratio 0.9%) • Quality average: 25.9% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:29:04	API Interceptor	1x Sleep call for process: wmaJOYGy7Q.exe modified
12:29:06	API Interceptor	887x Sleep call for process: RegAsm.exe modified
12:29:08	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegAsm.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.154	Updated Order COA.doc	Get hash	malicious	Browse	
	Maersk BL & PL.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	Qotation.exe	Get hash	malicious	Browse	
	SMJshb9rCD.exe	Get hash	malicious	Browse	
	3z4ibRIdCl.exe	Get hash	malicious	Browse	
	UfQ7WpbVPG.exe	Get hash	malicious	Browse	
	9ieQE1S5ZH.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealthybillionaire.ddns.net	Updated Order COA.doc	Get hash	malicious	Browse	• 185.140.53.154
	Revise Order Sheets.doc	Get hash	malicious	Browse	• 79.134.225.52
	TT SWIFT COPY.exe	Get hash	malicious	Browse	• 41.217.65.85
	bedrapes.exe	Get hash	malicious	Browse	• 154.118.68.3

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Updated Order COA.doc	Get hash	malicious	Browse	• 185.140.53.154
	Payment confirmation.exe	Get hash	malicious	Browse	• 185.140.53.45
	03soKqWLfN.exe	Get hash	malicious	Browse	• 185.140.53.145
	installer.exe	Get hash	malicious	Browse	• 185.140.53.145
	Maersk BL & PL.exe	Get hash	malicious	Browse	• 185.140.53.154
	vmw7WdkJ6k.exe	Get hash	malicious	Browse	• 185.140.53.12
	ORDER.exe	Get hash	malicious	Browse	• 185.140.53.135
	ORDER-21611docx.exe	Get hash	malicious	Browse	• 185.165.153.116
	6VYNUalwUt.exe	Get hash	malicious	Browse	• 185.244.30.92
	ORDER-6010.pdf.exe	Get hash	malicious	Browse	• 185.244.30.92
	CONTRACT.exe	Get hash	malicious	Browse	• 185.140.53.135
	doc0302732021052117330 5IMG0012.exe	Get hash	malicious	Browse	• 185.140.53.230
	yfilQwrYpA.exe	Get hash	malicious	Browse	• 185.140.53.216
	Ff6m4N8pog.exe	Get hash	malicious	Browse	• 185.140.53.216
	yCdBrRiAN2.exe	Get hash	malicious	Browse	• 185.140.53.216
	loKHQzx6Lf.exe	Get hash	malicious	Browse	• 185.140.53.216
	SecuriteInfo.com.Program.Win32.Wacapew.Cml.7225.exe	Get hash	malicious	Browse	• 185.140.53.129
	Shipping Documents_Bill of Lading 910571880.exe	Get hash	malicious	Browse	• 185.140.53.129
	knqh5Hw6gu.exe	Get hash	malicious	Browse	• 185.140.53.13
	Container_Deposit_slip_pdf.jar	Get hash	malicious	Browse	• 185.244.30.47

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	Trainer v22.3.exe	Get hash	malicious	Browse	
	Trainer v 4.6.1.exe	Get hash	malicious	Browse	
	PO 389293LC_pdf.exe	Get hash	malicious	Browse	
	qPyjO8F0ND.exe	Get hash	malicious	Browse	
	PAYMENT-PO#987654567.exe	Get hash	malicious	Browse	
	n3sQ7uTU8v.exe	Get hash	malicious	Browse	
	20014464370.PDF.exe	Get hash	malicious	Browse	
	aXgdOUvL9L.exe	Get hash	malicious	Browse	
	DHL#DOCUMENTS001010.PDF.exe	Get hash	malicious	Browse	
	kylfnzzg3E.exe	Get hash	malicious	Browse	
	flyZab7hHk.exe	Get hash	malicious	Browse	
	AedJpyQ9lM.exe	Get hash	malicious	Browse	
	UPDATED SOA.exe	Get hash	malicious	Browse	
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	
	RFQ27559404D4E5A.PDF.exe	Get hash	malicious	Browse	
	Receiptn.exe	Get hash	malicious	Browse	
	PURCHASE LIST.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.783.10804.exe	Get hash	malicious	Browse	
	Y6k2VgaGck.exe	Get hash	malicious	Browse	
	Bank swift.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\wmaJOYGy7Q.exe.log	
Process:	C:\Users\user\Desktop\wmaJOYGy7Q.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	**true**
Reputation:	moderate, 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,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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.Co

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\wmaJOYGy7Q.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070I
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Trainer v22.3.exe, Detection: malicious, Browse • Filename: Trainer v 4.6.1.exe, Detection: malicious, Browse • Filename: PO 389293LC_pdf.exe, Detection: malicious, Browse • Filename: qPyjO8F0ND.exe, Detection: malicious, Browse • Filename: PAYMENT-PO#987654567.exe, Detection: malicious, Browse • Filename: n3sQ7uTU8v.exe, Detection: malicious, Browse • Filename: 20014464370.PDF.exe, Detection: malicious, Browse • Filename: aXgdOUvL9L.exe, Detection: malicious, Browse • Filename: DHL#DOCUMENTS001010.PDF.exe, Detection: malicious, Browse • Filename: kyIfnzzg3E.exe, Detection: malicious, Browse • Filename: flyZab7hHk.exe, Detection: malicious, Browse • Filename: AedJpyQ9lM.exe, Detection: malicious, Browse • Filename: UPDATED SOA.exe, Detection: malicious, Browse • Filename: qdFDmi3Bhy.exe, Detection: malicious, Browse • Filename: RFQ27559404D4E5A.PDF.exe, Detection: malicious, Browse • Filename: Receiptn.exe, Detection: malicious, Browse • Filename: PURCHASE LIST.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.783.10804.exe, Detection: malicious, Browse • Filename: Y6k2VgaGck.exe, Detection: malicious, Browse • Filename: Bank swift.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o..... .*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o .....r]..p.o!....,..{T.....{U.....o"....+(.ra..p.o!.....,..{T.....

C:\Users\user\AppData\Local\Temp\tmp8A08.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1307
Entropy (8bit):	5.1055546710401485
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0aa5xtn:cbk4oL600QydbQxIYODOLedq3Ba5j
MD5:	E1762CDA6D6A3715B829E81B77FF06F7
SHA1:	B9F6318A5E4CDB1462E45A0B08EE46D303C40715
SHA-256:	48A86564D25864484ABE34BAA5B71890B8AF30ADE8AC1CF14BBACAE28036F09F
SHA-512:	DC6218645DBE168DCB8DE01124694FF26ED033E7A5CE066FAA1D00817F2E51D167938B4FF4231F514F60895EF0FFE95880D401358C69E49126A219CBF7D3E705
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	6.888016992762183
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRN/T8OpnPJS0zm+MW7OMVCUtOGouheflY838Ps:X4LDAnybgCFgwOpxS0T6MVXt7oVlYO80
MD5:	428943A5826E86C05E99C546AC9047A5
SHA1:	CA9F6226703DC0C08BA90B2D1AE600D65BC326B6
SHA-256:	9035E4EF869AAB276D3D53778202765133E9729234DA209C8F3EDFD1725ADDA9
SHA-512:	0A0EB940311463F56BF6ECD36D5ECC0FEC8838F7BFB71064600722B7AE656B92F46815DE5A5CF0B72072F7F5199B02BBE8BA562E4E98255BCF8F55331FE708DE
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S...X..:.....i...v.o{3.O....t.aQ.N.S..r.1w..akdp....._.H.;%g..7.N..R3$....jY....h.c..n.Q,.Y.W.].`..v....6.WI.l

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:9Qt:94
MD5:	EF699DB7839567D50C2DB9B9C2976141
SHA1:	163B8148EC1ABD31E6636DF6292F9359D63BF6EF
SHA-256:	6C45578026299778E2A8AA035587BF27ED6D59116FB0055848560E423691DF4D
SHA-512:	9B9D2AEE24DA97AB70AAA725A332B4CF4B656CEB41F1E84E13296C3080D090B4E38EBD1340E3B2DF10D447A0786BF2F4B03E5D4DD8828D84E64E3F7E9F9AED DB
Malicious:	**true**
Preview:	1.c..0.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.308768198567054
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAI0L4A:oNWXp+N23f0L4A
MD5:	C9298EEE68389B937EFD1A5CE3DB10A2
SHA1:	2D299BA869C5386FB114AA6016DCB0607DFE98E0
SHA-256:	270C3AC669C532CE18737BFD72CB2981B65A6F08FF2B7EB5C9A4D8834AEB4E62
SHA-512:	1EF5C4AC44E1658DC8EA56F98B2714297D39937B9817E4F843D067F59D2778EC3D65E34DD467442F8B7D86248813E834D47A71D79EC3CE2D8E54B8A41BF19FD
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Preview:	C:\Users\user\AppData\Local\Temp\RegAsm.exe

\Device\ConDrv	
Process:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	275
Entropy (8bit):	4.839531074781769
Encrypted:	false
SSDEEP:	6:z30qJ5tUI+30qobtUmYRZBXVNYL0dxKaRFfnYJin:z30mc30b4BFNY4xNYU
MD5:	1B648D405C15ECA8CF1B9B0469B5627E
SHA1:	C6BBAEDE7AE2353E15271F1FBAA18588BEF0E922
SHA-256:	52FF7329D9E47BF7366892E79338FEE702C60D1F3ADB2EDDB601DFAEC8F170A0
SHA-512:	086EC3F608C80CDB6DC844366CFBBA5237ABCEB5306C0EF7C91600003F1A169CD94EB07D3680E943C9AC498CBA3845857756C5D745A66999BE78C263E5C440
Malicious:	false
Preview:	Microsoft .NET Framework Assembly Registration Utility version 4.7.3056.0..for Microsoft .NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....RegAsm : error RA0000 : Unable to locate input assembly '0' or one of its dependencies...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.648738100237886
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	wmaJOYGy7Q.exe
File size:	659456
MD5:	5688c69c4379841eee42dcaec2dbf55a
SHA1:	09a30ec730d1fdf77e80f6d31aa4d810e36b1c44
SHA256:	62801897ae3411a8f144f2f7290ad2133ad0895f4f1550922dca9c6f4b9e8114
SHA512:	1cee75d6ffdc9a1e9e903672c83a7e042e9a6a34d42b156bd11a6ed215a82fe336e86158892a6ee129239f52f22ccfe19062d8668c6b9be5027775bd19424174
SSDEEP:	6144:ie7tkcyarn5KfNZCM2RG+zcwxOVbcEkXd5+d/T7xvoldaoAxKiYe1SvA5UamZ6vh:XFn5W8M4GSYbcb/+V7B+AcigemZ6Xd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....37B.....~'... ...@....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a277e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x4237339B [Tue Mar 15 19:12:27 2005 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa0784	0xa0800	False	0.623986930491	data	6.65837482247	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x394	0x400	False	0.375	data	2.92347158321	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/16/21-12:29:07.971503	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	5540	192.168.2.3	185.140.53.154
06/16/21-12:29:14.548582	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	5540	192.168.2.3	185.140.53.154

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:29:57.334021091 CEST	192.168.2.3	8.8.8.8	0x7918	Standard query (0)	wealthybil lionaire.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:30:13.983805895 CEST	192.168.2.3	8.8.8.8	0xd459	Standard query (0)	wealthybil lionaire.ddns.net	A (IP address)	IN (0x0001)
Jun 16, 2021 12:30:30.657831907 CEST	192.168.2.3	8.8.8.8	0x6d05	Standard query (0)	wealthybil lionaire.ddns.net	A (IP address)	IN (0x0001)

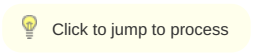
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:29:57.394704103 CEST	8.8.8.8	192.168.2.3	0x7918	No error (0)	wealthybil lionaire.ddns.net		185.140.53.154	A (IP address)	IN (0x0001)
Jun 16, 2021 12:30:14.042826891 CEST	8.8.8.8	192.168.2.3	0xd459	No error (0)	wealthybil lionaire.ddns.net		185.140.53.154	A (IP address)	IN (0x0001)
Jun 16, 2021 12:30:30.721060991 CEST	8.8.8.8	192.168.2.3	0x6d05	No error (0)	wealthybil lionaire.ddns.net		185.140.53.154	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: wmaJOYGy7Q.exe PID: 5344 Parent PID: 5792

General

Start time:	12:28:45
Start date:	16/06/2021
Path:	C:\Users\user\Desktop\wmaJOYGy7Q.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wmaJOYGy7Q.exe'
Imagebase:	0x190000
File size:	659456 bytes
MD5 hash:	5688C69C4379841EEE42DCAEC2DBF55A
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: 00000001.00000002.263955446.0000000003658000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.263955446.0000000003658000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.263955446.0000000003658000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.263784829.0000000003538000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.263784829.0000000003538000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.263784829.0000000003538000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.264154236.0000000003756000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.264154236.0000000003756000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.264154236.0000000003756000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 4764 Parent PID: 5344

General

Start time:	12:28:59
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0x7a0000
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: 00000005.00000002.481468397.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.481468397.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.481468397.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.490006265.0000000005050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.490006265.0000000005050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.490199362.0000000005250000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.490199362.0000000005250000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.490199362.0000000005250000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.486898144.00000000039B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.486898144.00000000039B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.484995497.0000000002971000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5812 Parent PID: 4764

General

Start time:	12:29:06
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8A08.tmp'
Imagebase:	0x1210000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1240 Parent PID: 5812

General

Start time:	12:29:06
Start date:	16/06/2021
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: RegAsm.exe PID: 6140 Parent PID: 528

General

Start time:	12:29:08
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe 0
Imagebase:	0xd0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6048 Parent PID: 6140

General

Start time:	12:29:08
Start date:	16/06/2021
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

Disassembly

Code Analysis