ID: 483799
Sample Name: wIQLBHYbqz
Cookbook: default.jbs
Time: 13:55:05
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

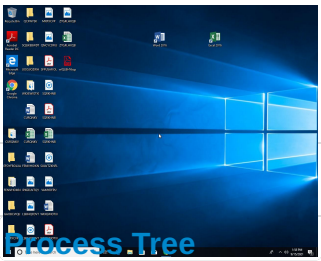
Windows Analysis Report wIQLBHYbqz

Overview

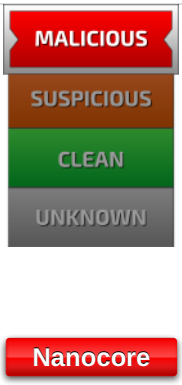
General Information

Sample Name:	wIQLBHYbqz (renamed file extension from none to exe)
Analysis ID:	483799
MD5:	1312d6ff22dbd8e..
SHA1:	913051c8f41e722.
SHA256:	543694f8b09a565.
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

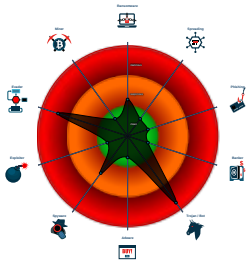


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected FrenchyShellcode packer
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…

Classification



- **System is w10x64**
- wIQLBHYbqz.exe (PID: 4904 cmdline: 'C:\Users\user\Desktop\wIQLBHYbqz.exe' MD5: 1312D6FF22DBD8E9E05D1B0D9130439D)
  - RegAsm.exe (PID: 4936 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe MD5: 529695608EAFBED00ACA9E61EF333A7C)
- RMActivate_isv.exe.bat (PID: 6788 cmdline: 'C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat' MD5: F9F1A2B23DF822033EC717757776CBB7)
  - RegAsm.exe (PID: 7040 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe MD5: 529695608EAFBED00ACA9E61EF333A7C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "0622add8-a38b-49c1-8dc8-c09cf432",
  "Group": "NewLappi",
  "Domain1": "megida.hopto.org",
  "Domain2": "",
  "Port": 8822,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.617258087.0000000005B70000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000D.00000002.617258087.0000000005B70000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000D.00000002.617258087.0000000005B70000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000003.581083346.000000000366 8000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x108f5:$x1: NanoCore.ClientPluginHost • 0x10932:$x2: IClientNetworkHost • 0x14465:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000003.581083346.000000000366 8000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 78 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.RegAsm.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
22.2.RegAsm.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
22.2.RegAsm.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
22.2.RegAsm.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfef5:$a: NanoCore 0xff05:$a: NanoCore 0x10139:$a: NanoCore 0x1014d:$a: NanoCore 0x1018d:$a: NanoCore 0xff54:$b: ClientPlugin 0x10156:$b: ClientPlugin 0x10196:$b: ClientPlugin 0x1007b:$c: ProjectData 0x10a82:$d: DESCrypto 0x1844e:$e: KeepAlive 0x1643c:$g: LogClientMessage 0x12637:$i: get_Connected 0x10db8:$j: #=q 0x10de8:$j: #=q 0x10e04:$j: #=q 0x10e34:$j: #=q 0x10e50:$j: #=q 0x10e6c:$j: #=q 0x10e9c:$j: #=q 0x10eb8:$j: #=q
13.2.RegAsm.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x1018d:$x1: NanoCore.ClientPluginHost 0x101ca:$x2: IClientNetworkHost 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 155 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Binary is likely a compiled AutoIt script file

AutoIt script contains suspicious strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Detected FrenchyShellcode packer

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

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

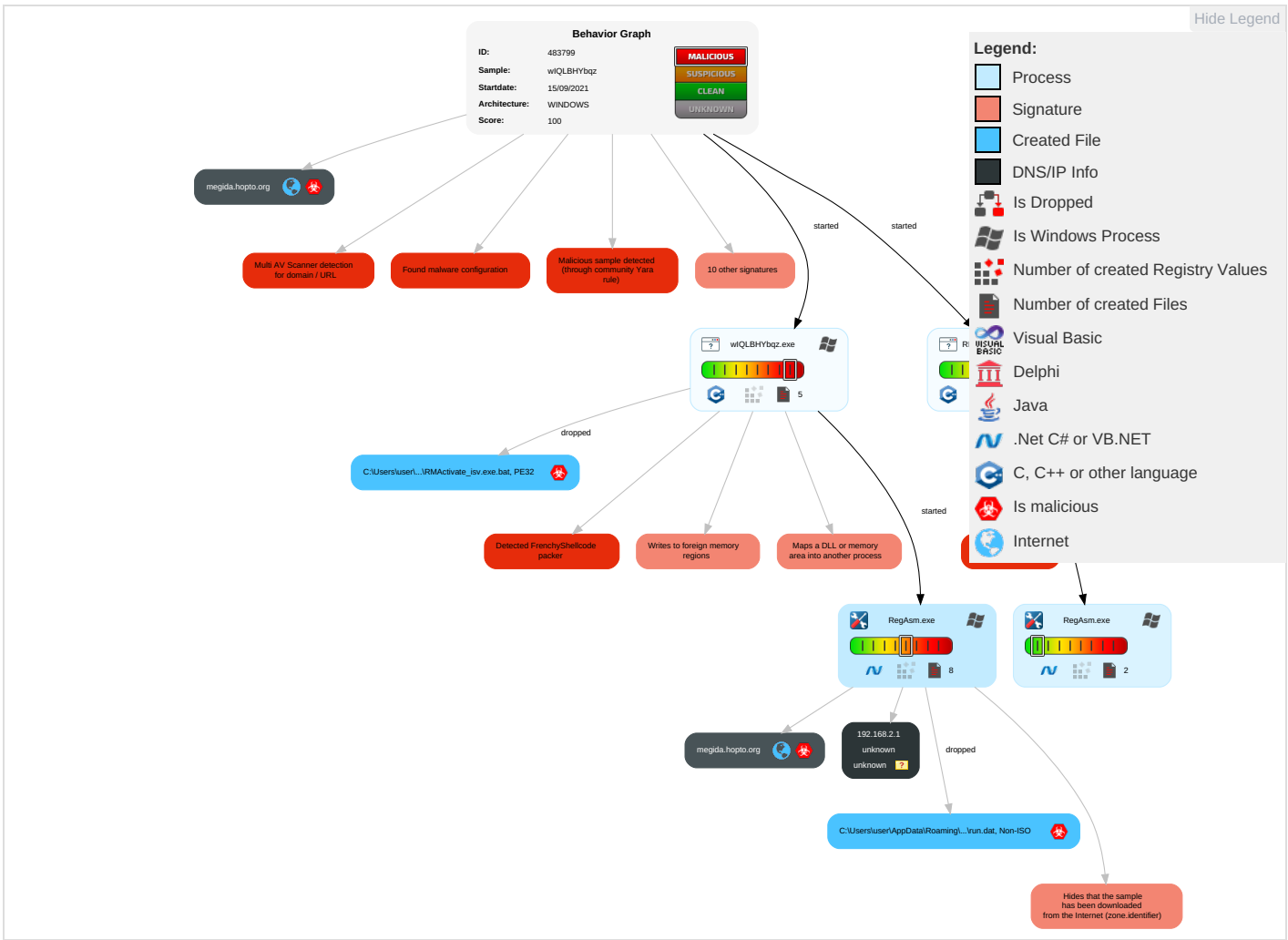
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Native API 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	Input Capture 3 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 3 1	Exfiltration Over Bluetooth	Remote Ac Software 1
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Obfuscated Files or Information 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2 1 2	Software Packing 2 1	NTDS	System Information Discovery 1 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transf Protocols

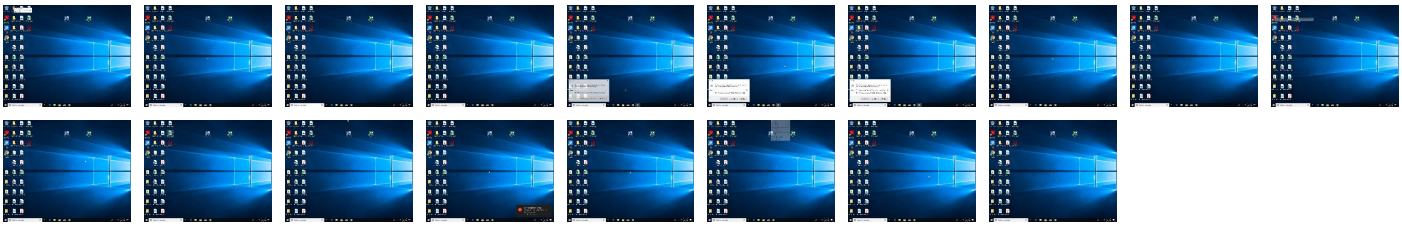
Behavior Graph



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
wlQLBHYbqz.exe	69%	Virustotal		Browse
wlQLBHYbqz.exe	63%	Metadefender		Browse
wlQLBHYbqz.exe	80%	ReversingLabs	Win32.Trojan.Skeeyah	
wlQLBHYbqz.exe	100%	Avira	HEUR/AGEN.1100005	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat	100%	Avira	HEUR/AGEN.1100005	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.wIQLBHYbqz.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
22.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.RegAsm.exe.5b70000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.0.RMActivate_isv.exe.bat.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
14.2.RMActivate_isv.exe.bat.16e0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.wIQLBHYbqz.exe.14a0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.wIQLBHYbqz.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
14.2.RMActivate_isv.exe.bat.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File

Domains

Source	Detection	Scanner	Label	Link
megida.hopto.org	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
megida.hopto.org	0%	Avira URL Cloud	safe	
http://checkip.dyndns.orgITime	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgDi	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
megida.hopto.org	0.0.0.0	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
megida.hopto.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483799
Start date:	15.09.2021
Start time:	13:55:05
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 8m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wIQLBHYbqz (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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/3@18/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.5%) • Quality average: 82.7% • Quality standard deviation: 10.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:56:55	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sdchange.lnk
13:57:02	API Interceptor	484x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
megida.hopto.org	vCVJO4xhuE.exe	Get hash	malicious	Browse	• 0.0.0.0
	SutRc8iT50.exe	Get hash	malicious	Browse	• 0.0.0.0
	BycT2K3tqw.exe	Get hash	malicious	Browse	• 0.0.0.0
	NaeJDbDEhv.exe	Get hash	malicious	Browse	• 0.0.0.0
	mKwRy5zlC1.exe	Get hash	malicious	Browse	• 0.0.0.0
	0b4KVMtyt2.exe	Get hash	malicious	Browse	• 0.0.0.0
	rMXtWZE8zC.exe	Get hash	malicious	Browse	• 0.0.0.0
	zKFX17X1HV.exe	Get hash	malicious	Browse	• 0.0.0.0
	iIfKHwYD3f.exe	Get hash	malicious	Browse	• 0.0.0.0
	8T2c71SMRc.exe	Get hash	malicious	Browse	• 0.0.0.0
	cdu4RCsVw5.exe	Get hash	malicious	Browse	• 0.0.0.0
	klRbC6ZYIH.exe	Get hash	malicious	Browse	• 0.0.0.0
	2gYXJQigWS.exe	Get hash	malicious	Browse	• 0.0.0.0
	FsYqgk2CFi.exe	Get hash	malicious	Browse	• 0.0.0.0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	w6OD0DrYr3.exe	Get hash	malicious	Browse	• 0.0.0.0
	TUtq51OHzM.exe	Get hash	malicious	Browse	• 0.0.0.0
	9DHL Package Delay Notification 20190614,pdf.exe	Get hash	malicious	Browse	• 194.5.98.25
	15Orascom Construction Limited Important Inquiry Document,pdf.exe	Get hash	malicious	Browse	• 194.5.98.25
	30Orascom Construction Company Limited Inquiry doc ument,pdf.exe	Get hash	malicious	Browse	• 194.5.98.25
	18CY.exe	Get hash	malicious	Browse	• 213.208.12 9.198

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:R7S8n:88
MD5:	5DDEC758B77D5B693053413AE49F06FA
SHA1:	102007D870F22E257D4B105971895F5FBA9303FD
SHA-256:	DFF20B05FF3AC595B9698967ED4E7862E19D377412984E30315660C021F11AD6
SHA-512:	50F0DD6357188F1E3406CD9374FF18FB92B4BBDAD37D7DDB9F759DAD639B2C4B7CCB4727C6414D953E51F11D5B89D323E9A025335E203C92AB8E21E495F26C0
Malicious:	**true**
Reputation:	low
Preview:	.*^.x.H

C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat

Process:	C:\Users\user\Desktop\wIQLBHYbqz.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1253984
Entropy (8bit):	7.161677576535402
Encrypted:	false
SSDEEP:	24576:9AHnh+eWsN3skA4RV1Hom2KXMmHaFZyrh9QI/C+EZCBqUIYXmf8MuvWzy:ch+ZkldoPK8YaFZyri7QPIYXLMK
MD5:	F9F1A2B23DF822033EC717757776CBB7
SHA1:	FFEFDCF1616F9A38EEC5EA269B911A070F0FCB06
SHA-256:	E6973E79CEC34C9DA0B10B28C95C28B5BF3F112216042E472CF40B6AF671E257
SHA-512:	99036EEF75098DF9247005DEF6D3F8646AEE382247E8E9558118F31167E4248F8B3EFB79343D09F431FC0672A227974E0DFFEAE92D7D4A23DA0B22AA4E3FB061
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..R...R...R....C..P....;.S..._@#.a..._@....._@..g...[j..[...[jo.w...R ...r.....#.S..._@'.S...R.k.S....".S...RichR.....PE..L.....\....."....<.....@.....@...@.....@.....@.....|.....x..... ..4q...+.....PK..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc....x.....z...4..... ..@..@.reloc..4q.....r.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sdchange.lnk	
Process:	C:\Users\user\Desktop\wIQLBHYbqz.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 15 19:56:51 2021, mtime=Wed Sep 15 19:56:51 2021, atime=Wed Sep 15 19:56:51 2021, length=1253984, window=hide
Category:	dropped
Size (bytes):	934
Entropy (8bit):	5.0399705120768425
Encrypted:	false
SSDEEP:	24:8o7bAJazTcb0domePeCVrKvHUeR/huyAH9i6/hAJ1m:8o7bAczQYd9ZCVkHvZsoqeJ1
MD5:	3A151859BF071B8B0A25E8778115EF19
SHA1:	7D6865050E2726091F4FC126267102BF8DCFB0B0
SHA-256:	D32FDF5749E8390DBD04933D2C8B118E3F312101D76ABCFDDA8D13F6D61F4ACF
SHA-512:	03D040B42E8E78E2B70AE1164051F9467FCF9A4E5BFAD0001CF4C70C8EBDFB648B15061D77460B98A3B3DD724AE2D7A7AC62E1FA545C9857165E66F8129FE46F
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....g.4t.....4t.....4t...`".....:...DG..Yr?.D..U..k0.&...&.....d.!-..Yc6%>.....5t.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N../S.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N../S.....Y.....D...R.o.a.m.i.n.g.....V.1...../S....Gfxv2_0.@...../S../S.....$H.....x.}.G.f.x.v.2._.0.....z.2.`"../S.. .RMACTI~1.BAT..^...../S../S.....%H.....Qt.R.M.A.c.t.i.v.a.t.e._.i.s.v...e.x.e...b.a.t.....o.....-.....n.....{.....C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat..-.....\....\....\....\....\.G.f.x.v.2._.0.\.R.M.A.c.t.i.v.a.t.e._.i.s.v...e.x.e...b.a.t.`.....X.....580913.....!a..%.H.VZAj..."...1.....-$..!a..%.H.VZAj..."...1.....-$.E.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.1616750530451565
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:	wIQLBHYbqz.exe
File size:	1253976
MD5:	1312d6ff22dbd8e9e05d1b0d9130439d
SHA1:	913051c8f41e722c522e637bdbdfa563ecfba4ff
SHA256:	543694f8b09a565a88932457d40d16cd85ac3f0b7be9ad322ef9486144379449
SHA512:	d16116efbbec351430dead1cc3c1a9029cb9781075bc7951ec2811c1b18962f3218cc1c308fe6bc7bc0dbdb3366a53926bef1f3bfdf78c236192e9af2890d740
SSDEEP:	24576:9AHnh+eWsN3skA4RV1Hom2KXMmHaFZyrh9QI/C+EZCBqUIYXmf8MuvWzr:ch+ZkldoPK8YaFZyri7QPIYXLMD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..R...R...R....C..P.....;.S..._@#.a..._@....._@..g...[j..[...[jo.w...R...r.....#.S..._@'.S...R.k.S.....".S...RichR..

File Icon

Icon Hash:	74e8cad0ccd4c4c4

Static PE Info

General

Entrypoint:	0x42800a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE

General

Time Stamp:	0x5CF61010 [Tue Jun 4 06:30:40 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	afcdf79be1557326c854b6e20cb900a7

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8dfdd	0x8e000	False	0.573560258033	data	6.67524835171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8f000	0x2fd8e	0x2fe00	False	0.328288185379	data	5.76324400576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xbf000	0x8f74	0x5200	False	0.10175304878	data	1.19638192355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x67804	0x67a00	False	0.94490255579	data	7.88902486537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x130000	0x7134	0x7200	False	0.575143914474	data	5.64336658125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	
French	France	

Static AutoIT Info

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 13:57:03.784324884 CEST	192.168.2.6	8.8.8.8	0x3282	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:07.895946026 CEST	192.168.2.6	8.8.8.8	0xaf8a	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:11.972706079 CEST	192.168.2.6	8.8.8.8	0x2f0b	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:16.216864109 CEST	192.168.2.6	8.8.8.8	0x222e	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:20.413863897 CEST	192.168.2.6	8.8.8.8	0xf245	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:24.694555044 CEST	192.168.2.6	8.8.8.8	0xf26d	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:28.968398094 CEST	192.168.2.6	8.8.8.8	0xa427	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:33.072887897 CEST	192.168.2.6	8.8.8.8	0xe0f	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:37.514784098 CEST	192.168.2.6	8.8.8.8	0xa946	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:41.604831934 CEST	192.168.2.6	8.8.8.8	0x5ce5	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:45.818428993 CEST	192.168.2.6	8.8.8.8	0xecc1	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:50.012881041 CEST	192.168.2.6	8.8.8.8	0x2d39	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:54.070163965 CEST	192.168.2.6	8.8.8.8	0x929c	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:58.353168011 CEST	192.168.2.6	8.8.8.8	0x9308	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:03.071388006 CEST	192.168.2.6	8.8.8.8	0x1425	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:07.313395023 CEST	192.168.2.6	8.8.8.8	0xda2	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:11.361876011 CEST	192.168.2.6	8.8.8.8	0x7d7c	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:15.394278049 CEST	192.168.2.6	8.8.8.8	0x3519	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 13:57:03.810755014 CEST	8.8.8.8	192.168.2.6	0x3282	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:07.925545931 CEST	8.8.8.8	192.168.2.6	0xaf8a	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:11.997688055 CEST	8.8.8.8	192.168.2.6	0x2f0b	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:16.249648094 CEST	8.8.8.8	192.168.2.6	0x222e	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:20.443173885 CEST	8.8.8.8	192.168.2.6	0xf245	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:24.723551989 CEST	8.8.8.8	192.168.2.6	0xf26d	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:29.004542112 CEST	8.8.8.8	192.168.2.6	0xa427	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:33.103174925 CEST	8.8.8.8	192.168.2.6	0xe0f	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:37.544377089 CEST	8.8.8.8	192.168.2.6	0xa946	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:41.634622097 CEST	8.8.8.8	192.168.2.6	0x5ce5	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 13:57:45.847418070 CEST	8.8.8.8	192.168.2.6	0xecc1	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:50.042393923 CEST	8.8.8.8	192.168.2.6	0x2d39	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:54.096656084 CEST	8.8.8.8	192.168.2.6	0x929c	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:57:58.383055925 CEST	8.8.8.8	192.168.2.6	0x9308	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:03.097934008 CEST	8.8.8.8	192.168.2.6	0x1425	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:07.342670918 CEST	8.8.8.8	192.168.2.6	0xda2	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:11.388569117 CEST	8.8.8.8	192.168.2.6	0x7d7c	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 13:58:15.423655987 CEST	8.8.8.8	192.168.2.6	0x3519	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wIQLBHYbqz.exe PID: 4904 Parent PID: 5288

General

Start time:	13:56:01
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\wIQLBHYbqz.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wIQLBHYbqz.exe'
Imagebase:	0x400000
File size:	1253976 bytes
MD5 hash:	1312D6FF22DBD8E9E05D1B0D9130439D
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: 00000000.00000003.453308954.000000000399F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.453308954.000000000399F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.453308954.000000000399F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.452029104.0000000003975000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.452029104.0000000003975000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.452029104.0000000003975000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.614883445.00000000014A2000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.614883445.00000000014A2000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.614883445.00000000014A2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.617706572.0000000003910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.617706572.0000000003910000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.617706572.0000000003910000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.450606191.0000000004911000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.450606191.0000000004911000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.450606191.0000000004911000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.617309688.0000000003893000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.617309688.0000000003893000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.617309688.0000000003893000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.450818264.000000000391C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.450818264.000000000391C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.450818264.000000000391C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.466877574.00000000039B2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.466877574.00000000039B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.466877574.00000000039B2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.618062231.0000000003997000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.618062231.0000000003997000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.618062231.0000000003997000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.618678183.0000000004910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.618678183.0000000004910000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.618678183.0000000004910000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegAsm.exe PID: 4936 Parent PID: 4904

General

Start time:	13:57:01
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Imagebase:	0xc50000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
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: 0000000D.00000002.617258087.0000000005B70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.617258087.0000000005B70000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.617258087.0000000005B70000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.609808438.0000000000402000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.609808438.0000000000402000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.609808438.0000000000402000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.615169994.0000000004247000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.615169994.0000000004247000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.616663037.00000000056F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.616663037.00000000056F0000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RMActivate_isv.exe.bat PID: 6788 Parent PID: 3440

General

Start time:	13:57:03
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat'

Imagebase:	0x400000
File size:	1253984 bytes
MD5 hash:	F9F1A2B23DF822033EC717757776CBB7
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: 0000000E.00000003.581083346.0000000003668000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.581083346.0000000003668000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.581083346.0000000003668000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000003.580718643.0000000003611000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.580718643.0000000003611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.580718643.0000000003611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.614749797.00000000016E2000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.614749797.00000000016E2000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.614749797.00000000016E2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000003.580844038.0000000003B80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.580844038.0000000003B80000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.580844038.0000000003B80000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000003.592051979.0000000003562000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.592051979.0000000003562000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.592051979.0000000003562000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000003.580617027.00000000035B9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.580617027.00000000035B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.580617027.00000000035B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000003.580586671.000000000369C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.580586671.000000000369C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.580586671.000000000369C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000003.580975519.000000000363C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000003.580975519.000000000363C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000003.580975519.000000000363C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: RegAsm.exe PID: 7040 Parent PID: 6788

General

Start time:	13:57:59
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Imagebase:	0x9d0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.611459498.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.611459498.0000000003081000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.609719074.0000000000402000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.609719074.0000000000402000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.609719074.0000000000402000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.611621495.0000000004081000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.611621495.0000000004081000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis