ID: 483610
Sample Name: vCVJO4xhuE
Cookbook: default.jbs
Time: 10:01:31
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

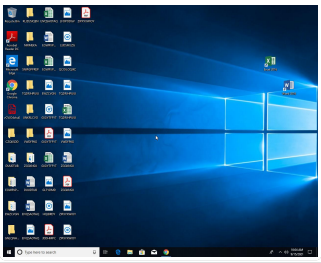
Windows Analysis Report vCVJO4xhuE

Overview

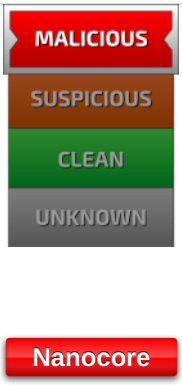
General Information

Sample Name:	vCVJO4xhuE (renamed file extension from none to exe)
Analysis ID:	483610
MD5:	2bc1291ce4bef39..
SHA1:	2d3b60943ddec9..
SHA256:	d0e91a9fb694973.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



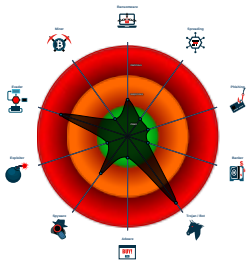
Nanocore

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…
- Writes to foreign memory regions
- Binary is likely a compiled AutoIt sc…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- vCVJO4xhuE.exe (PID: 2092 cmdline: 'C:\Users\user\Desktop\vCVJO4xhuE.exe' MD5: 2BC1291CE4BEF393A9407153D5E39640)
- RMActivate_isv.exe.bat (PID: 6600 cmdline: 'C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat' MD5: EE41C0FC7D593DE490C7C683B12CCA25)
  - RegAsm.exe (PID: 6680 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
00000017.00000002.518973202.000000000583 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000017.00000002.518973202.000000000583 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000010.00000002.519999032.0000000003A2 D000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10195:$x1: NanoCore.ClientPluginHost • 0x101d2:$x2: IClientNetworkHost • 0x13d05:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000010.00000002.519999032.0000000003A2 D000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000002.519999032.0000000003A2 D000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfefd:$a: NanoCore • 0xff0d:$a: NanoCore • 0x10141:$a: NanoCore • 0x10155:$a: NanoCore • 0x10195:$a: NanoCore • 0xff5c:$b: ClientPlugin • 0x1015e:$b: ClientPlugin • 0x1019e:$b: ClientPlugin • 0x10083:$c: ProjectData • 0x10a8a:$d: DESCrypto • 0x18456:$e: KeepAlive • 0x16444:$g: LogClientMessage • 0x1263f:$i: get_Connected • 0x10dc0:$j: #=q • 0x10df0:$j: #=q • 0x10e0c:$j: #=q • 0x10e3c:$j: #=q • 0x10e58:$j: #=q • 0x10e74:$j: #=q • 0x10ea4:$j: #=q • 0x10ec0:$j: #=q
Click to see the 83 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
16.3.RMActivate_isv.exe.bat.39c8b00.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
16.3.RMActivate_isv.exe.bat.39c8b00.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
16.3.RMActivate_isv.exe.bat.39c8b00.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
16.3.RMActivate_isv.exe.bat.39c8b00.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
16.3.RMActivate_isv.exe.bat.39c8b00.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 116 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:

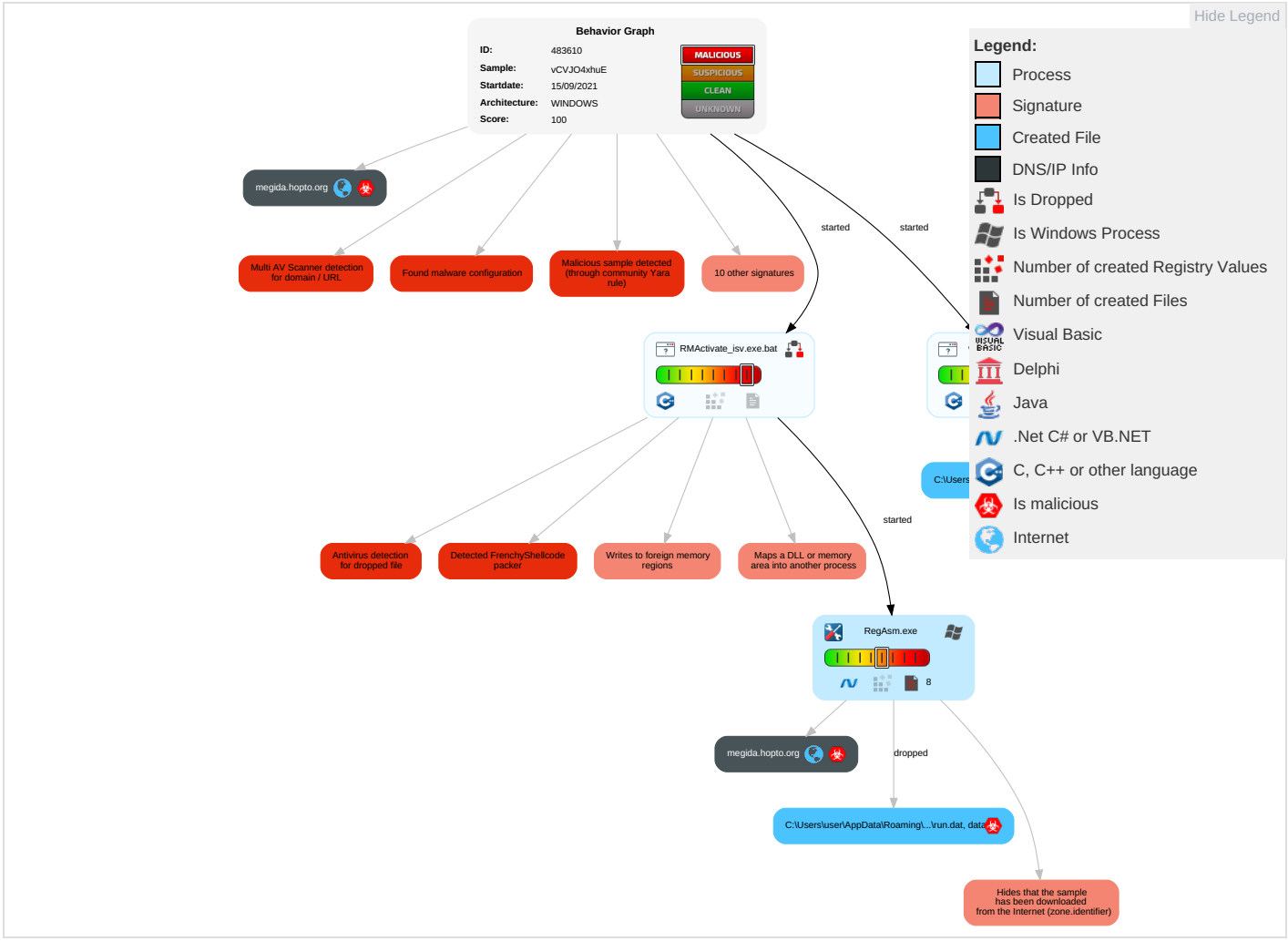
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation	Startup Items 1	Startup Items 1	Masquerading 1 1	Input Capture 3 1	System Time Discovery 1	Remote Services	Input Capture 3 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Remot Softwa
Domain Accounts	At (Linux)	DLL Side-Loading 1	Process Injection 2 1 2	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Process Injection 2 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

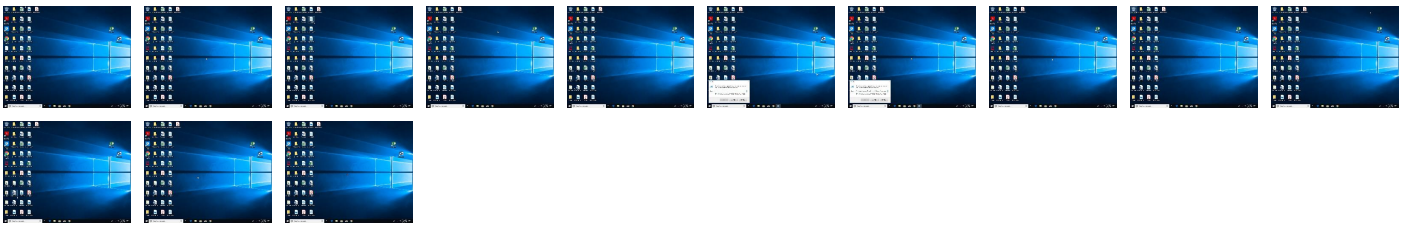
Behavior Graph



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
vCVJO4xhuE.exe	80%	ReversingLabs	Win32.Trojan.Skeeyah	
vCVJO4xhuE.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
16.2.RMActivate_isv.exe.bat.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
23.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.vCVJO4xhuE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
1.0.vCVJO4xhuE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
16.0.RMActivate_isv.exe.bat.400000.0.unpack	100%	Avira	HEUR/AGEN.1100005		Download File
16.2.RMActivate_isv.exe.bat.3150000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
23.2.RegAsm.exe.5db0000.7.unpack	100%	Avira	TR/NanoCore.fadte		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	12%	Virustotal		Browse
megida.hopto.org	0%	Avira URL Cloud	safe	
http://bot.whatismyipaddress.comc=	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgL	0%	Avira URL Cloud	safe	
http://bot.whatismyipaddress.comU	0%	Avira URL Cloud	safe	
http://checkip.dyndns.orgmTimeq	0%	Avira URL Cloud	safe	
http://checkip.dyndns.orgmTime	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	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483610
Start date:	15.09.2021
Start time:	10:01:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vCVJO4xhuE (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:	24
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@104/3@4/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 89% • Quality standard deviation: 0%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:03:21	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sdchange.lnk
10:04:26	API Interceptor	68x 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	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
	ilfKHwYD3f.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
	kIRbC6ZYIH.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
	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 document,pdf.exe	Get hash	malicious	Browse	• 194.5.98.25
	18CY.exe	Get hash	malicious	Browse	• 213.208.129.198
	55DHL Delayed Parcel Notification Document 201904124 Print,pdf.exe	Get hash	malicious	Browse	• 185.247.228.13

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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	CFC8B736D4B9C6C27D8CC12606D2B491
SHA1:	0A79518BEDAA1EEA5A87FDE2DA5F50716C59B62A
SHA-256:	4AE1CA3EDE339DAAC910A86E66F4FAA03C984177B92EF6E080F6A8B854BC0AF4
SHA-512:	336B11F9B2C68D1F4ECB1B6609101678FBECDFB3968AFB4BBB1B9D3A665898597D31A7579BC47D2A14A69A67FB59FF20334470A09966C93A25B545BEC04A12F
Malicious:	**true**
Reputation:	low
Preview:	....jx.H

C:\Users\user\AppData\Roaming\Gfxv2_0\RMActivate_isv.exe.bat	
Process:	C:\Users\user\Desktop\vCVJO4xhuE.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1254056
Entropy (8bit):	7.161673872850711
Encrypted:	false
SSDEEP:	24576:9AHnh+eWsN3skA4RV1Hom2KXMmHaFZyrh9QI/C+EZCBqUIYXmf8MuvWze:ch+ZkldoPK8YaFZyri7QPIYXLMG
MD5:	EE41C0FC7D593DE490C7C683B12CCA25
SHA1:	4B451F5F14AEAD1F0A5DD2C49607751012811C39
SHA-256:	8918686EA8D8BC111FE877795392EBE6838A17B30B95102D72A9CA8E1FBB10CA
SHA-512:	56E7C9A1993155974554757192D9BE041307C8BE159272E722B242766CFF8BC825C8EB3713647EFC30BD1A3E9DD80A108872EBCDB76D1F881BA4A80B29925C9
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\vCVJO4xhuE.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 15 16:03:18 2021, mtime=Wed Sep 15 16:03:18 2021, atime=Wed Sep 15 16:03:18 2021, length=1254056, window=hide
Category:	dropped
Size (bytes):	932
Entropy (8bit):	5.055848816493263
Encrypted:	false
SSDEEP:	12:8g1w4BTjCof7KwY//i0f7T5eLe/PvH5KoVY2gKHssFwEjEjAjVHmi9g/sFwjRbnm:8gbxFf+3q0faeRKLeMhEUAci6/hZm
MD5:	78433265C2E2CEEC888298F412113607
SHA1:	8649F7BD7230AA396AE87228F53F3CEF8B21D443
SHA-256:	DCE34A53294DD66E2ED00CF4BD4DB6692F4996EA4651F1AE98E78E27CD7D30EA
SHA-512:	5C8AB029631E7C3C5084959F87F1E68861A5101F0FAAC7885F90611EC18423BE2CBAD613A4F3A30B17B650942AFB7F6A87F3E6B6422C990888B74B6179679 62B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sdchange.lnk	
Preview:	L.....F.... ....=..S....e..S....e..S...."..... :...DG..Yr?.D..U..k0.&...&.....-..4...8.....S.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(.....gVA.G..k...@ .....NM./SH.....Y.....R..A.p.p.D.a.t.a...B.V.1.....NN...Roaming.@.....NM./SH.....Y.....f...R.o.a.m.i.n.g.....V.1...../Sj...Gfxv2_0.@...../Sj./Sj...._..... .....E~..G.f.x.v.2._.0.....z.2.."../Sj. .RMACTI~1.BAT..^...../Sj./Sj....-.....wV..R.M.A.c.t.i.v.a.t.e._.i.s.v...e.x.e...b.a.t.....m.....-.....l.....}.....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.....216554.....!a..%.H.VZAj. ...et.+.....W...!a..%.H.VZAj....et.+.....W..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):	7.161670518078121
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:	vCVJO4xhuE.exe
File size:	1254048
MD5:	2bc1291ce4bef393a9407153d5e39640
SHA1:	2d3b60943ddec9126b6b8f3e038538f2816573ad
SHA256:	d0e91a9fb694973c0c69180751710002db2a7c6e9cdbd47c934db3d15d0237f8
SHA512:	bfc29806df7b43717af4db144c0c7575d4b306a597a87acd4b85bfc55b29b7eff43b0e97c07313d2be4a52a72469131bae3b2c29a401e943eee7b31f94c053ed
SSDEEP:	24576:9AHnh+eWsN3skA4RV1Hom2KXMmHaFZyrh9QI/C+EZCBqUIYXmf8MuvWzF:ch+ZkldoPK8YaFZyri7QPIYXLMN
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
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 10:04:28.665054083 CEST	192.168.2.5	8.8.8.8	0x2168	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:04:32.807542086 CEST	192.168.2.5	8.8.8.8	0xd21e	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:04:36.894678116 CEST	192.168.2.5	8.8.8.8	0xecdc	Standard query (0)	megida.hopto.org	A (IP address)	IN (0x0001)
Sep 15, 2021 10:04:40.942200899 CEST	192.168.2.5	8.8.8.8	0x88df	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 10:04:28.703587055 CEST	8.8.8.8	192.168.2.5	0x2168	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 10:04:32.844679117 CEST	8.8.8.8	192.168.2.5	0xd21e	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 10:04:36.926017046 CEST	8.8.8.8	192.168.2.5	0xecdc	No error (0)	megida.hopto.org		0.0.0.0	A (IP address)	IN (0x0001)
Sep 15, 2021 10:04:40.970097065 CEST	8.8.8.8	192.168.2.5	0x88df	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: vCVJO4xhuE.exe PID: 2092 Parent PID: 360

General

Start time:	10:02:29
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\vCVJO4xhuE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vCVJO4xhuE.exe'
Imagebase:	0x400000
File size:	1254048 bytes
MD5 hash:	2BC1291CE4BEF393A9407153D5E39640
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: 00000001.00000003.389394525.0000000004A04000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389394525.0000000004A04000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389394525.0000000004A04000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.354701395.00000000035BF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.354701395.00000000035BF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.354701395.00000000035BF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.389514624.000000000351B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389514624.000000000351B000.00000004.00000001.sdmp, Author: Joe Security

- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389514624.000000000351B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.367225592.0000000003616000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.367225592.0000000003616000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.367225592.0000000003616000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.395699656.00000000049D1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.395699656.00000000049D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.395699656.00000000049D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.389323805.0000000003616000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389323805.0000000003616000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389323805.0000000003616000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.389092222.0000000004A88000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389092222.0000000004A88000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389092222.0000000004A88000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.354522815.00000000049D1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.354522815.00000000049D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.354522815.00000000049D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.389257286.0000000003616000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389257286.0000000003616000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389257286.0000000003616000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.389450364.0000000003616000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389450364.0000000003616000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389450364.0000000003616000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.389139947.0000000003652000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.389139947.0000000003652000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.389139947.0000000003652000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.354907425.00000000035EA000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.354907425.00000000035EA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.354907425.00000000035EA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.354551244.0000000003567000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.354551244.0000000003567000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 00000001.00000003.354551244.0000000003567000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: RMActivate_isv.exe.bat PID: 6600 Parent PID: 3472

General

Start time:	10:03:29
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:	1254056 bytes
MD5 hash:	EE41C0FC7D593DE490C7C683B12CCA25
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: 00000010.00000002.519999032.0000000003A2D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.519999032.0000000003A2D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.519999032.0000000003A2D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.520088685.0000000003B0C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.520088685.0000000003B0C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.520088685.0000000003B0C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.479677997.0000000003919000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.479677997.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.479677997.0000000003919000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.479626699.00000000039FC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.479626699.00000000039FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.479626699.00000000039FC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.479800874.0000000003971000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.479800874.0000000003971000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.479800874.0000000003971000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.519335292.0000000003152000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.519335292.0000000003152000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.519335292.0000000003152000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.480082743.00000000039C8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.480082743.00000000039C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.480082743.00000000039C8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.519568407.000000000388E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.519568407.000000000388E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.519568407.000000000388E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.479988416.000000000399C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.479988416.000000000399C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.479988416.000000000399C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.519893477.0000000003914000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.519893477.0000000003914000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.519893477.0000000003914000.00000004.00000001.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: 6680 Parent PID: 6600

General

Start time:	10:04:25
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:	0xe90000
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: 00000017.00000002.518973202.0000000005830000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000017.00000002.518973202.0000000005830000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.513670945.0000000000402000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.513670945.0000000000402000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.513670945.0000000000402000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.518307400.0000000004563000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.518307400.0000000004563000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.519204107.0000000005DB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000017.00000002.519204107.0000000005DB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.519204107.0000000005DB0000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis