ID: 431751
Sample Name: kylfnzzg3E.exe
Cookbook: default.jbs
Time: 08:47:15
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

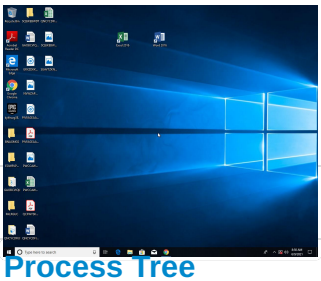
Analysis Report kyIfnzzg3E.exe

Overview

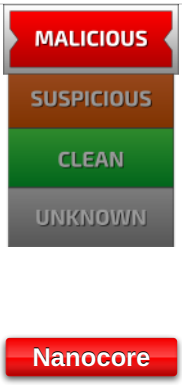
General Information

Sample Name:	kyIfnzzg3E.exe
Analysis ID:	431751
MD5:	eb43b3c033bd76..
SHA1:	0d39ffcf64ed4f38..
SHA256:	4e9a5cc90f1d175..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

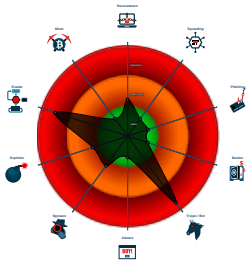


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Creates an undocumented autostart …

Classification



Process Tree

- **System is w10x64**
- kyIfnzzg3E.exe (PID: 5860 cmdline: 'C:\Users\user\Desktop\kyIfnzzg3E.exe' MD5: EB43B3C033BD76B51B90A51A6726A81C)
  - RegAsm.exe (PID: 3636 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 4276 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "4614bd42-26c0-4da0-8e09-16890d37",
  "Group": "Default",
  "Domain1": "wekeepworking.sytes.net",
  "Domain2": "wekeepworking12.sytes.net",
  "Port": 1144,
  "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

Initial Sample

Source	Rule	Description	Author	Strings
kyIfnzzg3E.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\win33.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.250699387.00000000001D2000.00000002.00020000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000007.00000002.461789098.00000000004020000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.461789098.00000000004020000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.461789098.000000000402000.00000040.00000001.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
00000000.00000002.251456849.000000000256000.00000004.00000001.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.RegAsm.exe.400000.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
7.0.RegAsm.exe.400000.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
7.0.RegAsm.exe.400000.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
7.0.RegAsm.exe.400000.3.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
0.0.kyIfnzzg3E.exe.1d0000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 39 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 domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Yara detected Costura Assembly Loader

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

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:

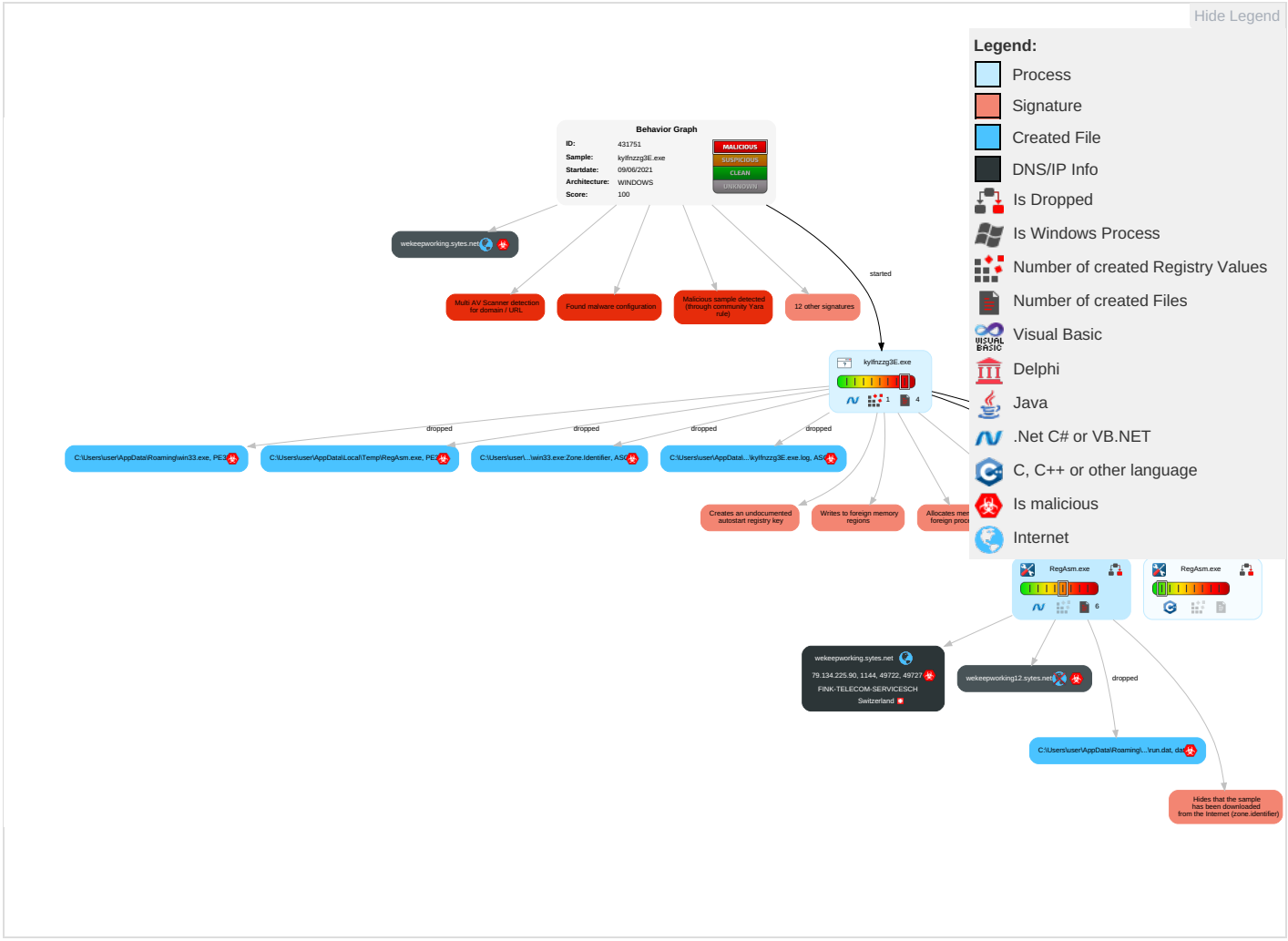
Detected Nanocore Rat

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	Networl Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 3 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Networl Commu
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirec Calls/SM
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	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Car 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 1 1	Manipul Device Commu
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	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco
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 St

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
kylfnzzg3E.exe	39%	Virustotal		Browse
kylfnzzg3E.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
kylfnzzg3E.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\win33.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\win33.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.RegAsm.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
wekeepworking.sytes.net	8%	Virustotal		Browse
wekeepworking12.sytes.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
wekeepworking.sytes.net	8%	Virustotal		Browse
wekeepworking.sytes.net	0%	Avira URL Cloud	safe	
wekeepworking12.sytes.net	2%	Virustotal		Browse
wekeepworking12.sytes.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wekeepworking.sytes.net	79.134.225.90	true	true	• 8%, Virustotal, Browse	unknown
wekeepworking12.sytes.net	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wekeepworking.sytes.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
wekeepworking12.sytes.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.90	wekeepworking.sytes.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431751
Start date:	09.06.2021
Start time:	08:47:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kylfnzzg3E.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:	27
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@5/5@39/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 3.5%) • Quality average: 54.1% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:48:28	API Interceptor	867x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.90	Ref 0180066743.xlsx	Get hash	malicious	Browse	
	AedJpyQ9lM.exe	Get hash	malicious	Browse	
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	
	A2PlnLyOA7.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	
	LOT_20210526.xlsx	Get hash	malicious	Browse	
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	
	4fn66P5vkl.exe	Get hash	malicious	Browse	
	P_O 00041221.xlsx	Get hash	malicious	Browse	
	LOT_20210526.xlsx	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wekeepworking.sytes.net	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90
	A2PlnLyOA7.exe	Get hash	malicious	Browse	• 79.134.225.90
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	• 79.134.225.90
	4fn66P5vkl.exe	Get hash	malicious	Browse	• 79.134.225.90
	P_O 00041221.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QI5MR3pte0.exe	Get hash	malicious	Browse	• 185.140.53.40
	5Em2NXNxSt.exe	Get hash	malicious	Browse	• 185.140.53.40
	7Zpsd899Kf.exe	Get hash	malicious	Browse	• 185.140.53.40
	LfgEatrwIF.exe	Get hash	malicious	Browse	• 185.140.53.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	MS2106071066.exe	Get hash	malicious	Browse	• 79.134.225.71
	Kangean PO.doc	Get hash	malicious	Browse	• 79.134.225.72
	facture.jar	Get hash	malicious	Browse	• 79.134.225.69
	c3yBu1IF57.exe	Get hash	malicious	Browse	• 79.134.225.92
	DPSGNwkO1Z.exe	Get hash	malicious	Browse	• 79.134.225.25
	SecuriteInfo.com.Trojan.Win32.Save.a.16917.exe	Get hash	malicious	Browse	• 79.134.225.94
	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	H538065217Invoice.exe	Get hash	malicious	Browse	• 79.134.225.9
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	P.I-84512.doc	Get hash	malicious	Browse	• 79.134.225.41
	l00VLAF9y0xQ9Vr.exe	Get hash	malicious	Browse	• 79.134.225.92
	Swift [ref QT #U2013 2102001-R2]pdf.exe	Get hash	malicious	Browse	• 79.134.225.10
	PO756654.exe	Get hash	malicious	Browse	• 79.134.225.99
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90
	br.exe	Get hash	malicious	Browse	• 79.134.225.73
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 79.134.225.71
	as.exe	Get hash	malicious	Browse	• 79.134.225.73
	11.exe	Get hash	malicious	Browse	• 79.134.225.40
	V8IB839cvz.exe	Get hash	malicious	Browse	• 79.134.225.25

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	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	
	tT1XWdxOYv.exe	Get hash	malicious	Browse	
	363IN050790620 BOOKING.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	RFQ#21040590409448.pdf.exe	Get hash	malicious	Browse	
	DHL#DOCUMENTS02010910.PDF.exe	Get hash	malicious	Browse	
	QOUTATION#2300003590.PDF.exe	Get hash	malicious	Browse	
	1p037oXV3S.exe	Get hash	malicious	Browse	
	BaU9m8mMFx.exe	Get hash	malicious	Browse	
	yl77tM4JDg.exe	Get hash	malicious	Browse	
	Payment Advice Reference0000 docx.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kyIfnzzg3E.exe.log

Process:	C:\Users\user\Desktop\kyIfnzzg3E.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kyIfnzzg3E.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\kyIfnzzg3E.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: 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 • Filename: tT1XWdxOYv.exe, Detection: malicious, Browse • Filename: 363IN050790620 BOOKING.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: RFQ#21040590409448.pdf.exe, Detection: malicious, Browse • Filename: DHL#DOCUMENTS02010910.PDF.exe, Detection: malicious, Browse • Filename: QOUTATION#2300003590.PDF.exe, Detection: malicious, Browse • Filename: 1p037oXV3S.exe, Detection: malicious, Browse • Filename: BaU9m8mMFx.exe, Detection: malicious, Browse • Filename: yl77tM4JDg.exe, Detection: malicious, Browse • Filename: Payment Advice Reference0000 docx.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.rI..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\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:mFn:mFn
MD5:	945B90EA6AB1D08300EFEDF91C6CF420
SHA1:	4005449440FA1F4CB80CBAAD1696EE772B146466
SHA-256:	8216AC6AE2A35895233B0689C5A16B4AF33A03BBA6926523BC015B50F950C8CB

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-512:	B263F02367AF88FE208B3D365FEC89649F4916D55C8691704CD2DB59B3C91848CB2D2480CF1D0247FBDFCD89FD37C6DF6BE0A548CD4235A3056F6F5E240AD2
Malicious:	**true**
Reputation:	low
Preview:	.&.^+.H

C:\Users\user\AppData\Roaming\win33.exe	
Process:	C:\Users\user\Desktop\kyIfnzzg3E.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	734208
Entropy (8bit):	7.833756558737052
Encrypted:	false
SSDEEP:	12288:iRqIue16rc2fV5hZcK1KjkiZCx7jsFuR6Y/ctiBHkcpZtoMZ:AqIue1kff/ECKwiZCx34mcC9LtoMZ
MD5:	EB43B3C033BD76B51B90A51A6726A81C
SHA1:	0D39FFCF64ED4F38EA83A72D726D40881F583014
SHA-256:	4E9A5CC90F1D17550208942E0182E9A99598C18C19B3467C184A46F4214755E2
SHA-512:	7EFB598153F2C4760FE17F7EF6510F5A48482027434B303A93439BD4C472C3D4E676E3BB8AED268277696F834DC93EA8853481D94C5FACAF61BECF4A23C17A8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Roaming\win33.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....(.....G... ...`....@.. ..... .@.....PG..K....`..`..... ....H.....text....'... ...(..... ..`.rsrc...`....`.....*.....@..@.reloc..... .....2.....@..B.....G.....H.....S.. ;.....2.....0..... .....8.....E....}...).....I.....8x...(....8....8t... ....~....9....&8.....:4... ....~a...:....& ....8....8/... ....~{...:....&8....(.... ....~*...9p...&8f....:....8....*8....8.....*....(....*..(0...*&~.....*...~....*..0..t.....(.... ....~!...:....& ....8....8.....E.... .....8....*8.... ....~q...:....&8.....9... .&&8....8....}....8....~...9....8....&{....8....&8....*~...

C:\Users\user\AppData\Roaming\win33.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\kyIfnzzg3E.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.833756558737052
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	kyIfnzzg3E.exe
File size:	734208
MD5:	eb43b3c033bd76b51b90a51a6726a81c
SHA1:	0d39ffcf64ed4f38ea83a72d726d40881f583014

General

SHA256:	4e9a5cc90f1d17550208942e0182e9a99598c18c19b3467c184a46f4214755e2
SHA512:	7efb598153f2c4760fe17f7ef6510f5a48482027434b303a93439bd4c472c3d4e676e3bb8aed268277696f834dc93ea8853481d94c5facaf61becf4a23c17a8c
SSDEEP:	12288:iRqIue16rc2fV5hZcK1KjkiZCx7jsFuR6Y/ctiBHkcpZtoMZ:AqIue1kff/ECKwiZCx34mcC9LtoMZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....(.....G... ...`....@.. .....@.....

File Icon

Icon Hash:	5cd0e8ccc4ec30f0

Static PE Info

General

Entrypoint:	0x4a479e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60BFED7F [Tue Jun 8 22:21:51 2021 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	0xa27a4	0xa2800	False	0.982952223558	data	7.98582259438	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x10760	0x10800	False	0.387976444129	data	4.61292982657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	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

Network Port Distribution

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 08:48:30.427062035 CEST	192.168.2.3	8.8.8.8	0x6606	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:35.760768890 CEST	192.168.2.3	8.8.8.8	0xd85b	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:41.134452105 CEST	192.168.2.3	8.8.8.8	0xb68c	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:46.537439108 CEST	192.168.2.3	8.8.8.8	0xe399	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:46.586323977 CEST	192.168.2.3	8.8.4.4	0x6e14	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:46.871432066 CEST	192.168.2.3	8.8.8.8	0xdd80	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:50.960513115 CEST	192.168.2.3	8.8.8.8	0xbe2	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:51.007548094 CEST	192.168.2.3	8.8.4.4	0xb17b	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:51.203886032 CEST	192.168.2.3	8.8.8.8	0x829b	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:55.272496939 CEST	192.168.2.3	8.8.8.8	0x9c83	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:55.339243889 CEST	192.168.2.3	8.8.4.4	0x62ee	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:55.504285097 CEST	192.168.2.3	8.8.8.8	0xc4bd	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:59.616060019 CEST	192.168.2.3	8.8.8.8	0xe6d2	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:04.839395046 CEST	192.168.2.3	8.8.8.8	0xdf04	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:10.071288109 CEST	192.168.2.3	8.8.8.8	0xb5c1	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:15.360275030 CEST	192.168.2.3	8.8.8.8	0xd49c	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:15.408368111 CEST	192.168.2.3	8.8.4.4	0xced3	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:15.927696943 CEST	192.168.2.3	8.8.8.8	0xfbfb	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:20.106766939 CEST	192.168.2.3	8.8.8.8	0x1a3a	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:20.180037022 CEST	192.168.2.3	8.8.4.4	0x1c99	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:20.445542097 CEST	192.168.2.3	8.8.8.8	0x2e3d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:24.537130117 CEST	192.168.2.3	8.8.8.8	0xbd14	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:24.583209038 CEST	192.168.2.3	8.8.4.4	0x4ec6	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:24.668420076 CEST	192.168.2.3	8.8.8.8	0xb5cd	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:28.791361094 CEST	192.168.2.3	8.8.8.8	0x1c05	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:34.405328989 CEST	192.168.2.3	8.8.8.8	0x3c9a	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:39.757822990 CEST	192.168.2.3	8.8.8.8	0xe0fd	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:45.137665987 CEST	192.168.2.3	8.8.8.8	0xacaa	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:45.314492941 CEST	192.168.2.3	8.8.4.4	0xcd5e	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:45.404165030 CEST	192.168.2.3	8.8.8.8	0xa24d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 08:49:49.507503986 CEST	192.168.2.3	8.8.8.8	0x4193	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:49.654870033 CEST	192.168.2.3	8.8.4.4	0x4bed	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:49.770097017 CEST	192.168.2.3	8.8.8.8	0x1078	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:53.939744949 CEST	192.168.2.3	8.8.8.8	0xee6d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:53.990129948 CEST	192.168.2.3	8.8.4.4	0xa85	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:54.121324062 CEST	192.168.2.3	8.8.8.8	0x1e1	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:58.202971935 CEST	192.168.2.3	8.8.8.8	0x69ea	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:50:03.425534964 CEST	192.168.2.3	8.8.8.8	0x6344	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 08:50:08.665294886 CEST	192.168.2.3	8.8.8.8	0x5e12	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 08:48:30.474170923 CEST	8.8.8.8	192.168.2.3	0x6606	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:35.807027102 CEST	8.8.8.8	192.168.2.3	0xd85b	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:41.179805994 CEST	8.8.8.8	192.168.2.3	0xb68c	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:48:59.659225941 CEST	8.8.8.8	192.168.2.3	0xe6d2	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:04.882405996 CEST	8.8.8.8	192.168.2.3	0xdf04	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:10.115674973 CEST	8.8.8.8	192.168.2.3	0xb5c1	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:28.834433079 CEST	8.8.8.8	192.168.2.3	0x1c05	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:34.447954893 CEST	8.8.8.8	192.168.2.3	0x3c9a	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:39.803596020 CEST	8.8.8.8	192.168.2.3	0xe0fd	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:49:58.247427940 CEST	8.8.8.8	192.168.2.3	0x69ea	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:50:03.472016096 CEST	8.8.8.8	192.168.2.3	0x6344	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 08:50:08.709853888 CEST	8.8.8.8	192.168.2.3	0x5e12	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: kyIfnzzg3E.exe PID: 5860 Parent PID: 5616

General

Start time:	08:47:59
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\kyIfnzzg3E.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\kyIfnzzg3E.exe'
Imagebase:	0x1d0000
File size:	734208 bytes
MD5 hash:	EB43B3C033BD76B51B90A51A6726A81C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.250699387.00000000001D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.251456849.0000000002561000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.252649732.00000000037D6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.252649732.00000000037D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.252649732.00000000037D6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000000.194675696.00000000001D2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.251887619.0000000003645000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.251887619.0000000003645000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.251887619.0000000003645000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.251765887.0000000003561000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.251765887.0000000003561000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.251765887.0000000003561000.00000004.00000001.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

Key Value Created

Analysis Process: RegAsm.exe PID: 3636 Parent PID: 5860

General

Start time:	08:48:24
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0xa0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

Analysis Process: RegAsm.exe PID: 4276 Parent PID: 5860

General

Start time:	08:48:24
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0xbf0000
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: 00000007.00000002.461789098.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.461789098.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.461789098.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.249612191.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.249612191.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.249612191.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.249317743.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.249317743.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.249317743.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis