ID: 431593
Sample Name: c3yBu1IF57.exe
Cookbook: default.jbs
Time: 00:14:22
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

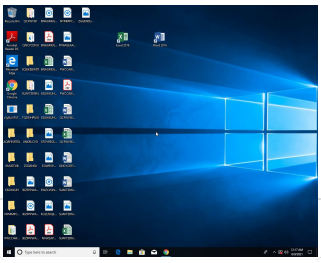
Analysis Report c3yBu1IF57.exe

Overview

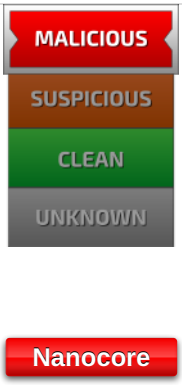
General Information

Sample Name:	c3yBu1IF57.exe
Analysis ID:	431593
MD5:	04f4a27d282ec9e.
SHA1:	8b8f849c58baa0b.
SHA256:	4da007eb010d6b..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



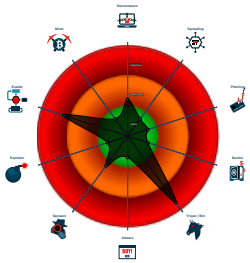
Nanocore

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- c3yBu1IF57.exe (PID: 5564 cmdline: 'C:\Users\user\Desktop\c3yBu1IF57.exe' MD5: 04F4A27D282EC9EA66549F35B6FF0559)
  - schtasks.exe (PID: 5408 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp24AD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- c3yBu1IF57.exe (PID: 6080 cmdline: C:\Users\user\Desktop\c3yBu1IF57.exe 0 MD5: 04F4A27D282EC9EA66549F35B6FF0559)
- **cleanup**

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2021

```
{
  "Version": "1.2.2.0",
  "Mutex": "aa01ad7d-c4c6-4050-b975-9fe8a3c1",
  "Group": "SPK#0998",
  "Domain1": "sawitupnew.expackplc.club",
  "Domain2": "sawitupnew.expackplc.club",
  "Port": 44322,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
c3yBu1IF57.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
c3yBu1IF57.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
c3yBu1IF57.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
c3yBu1IF57.exe	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

Copyright Joe Security LLC 2021

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.204561377.00000000003B2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000000.204561377.00000000003B2000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000000.204561377.00000000003B2000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000005.00000002.219125636.000000000297 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.219125636.000000000297 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2396f:$a: NanoCore • 0x239c8:$a: NanoCore • 0x23a05:$a: NanoCore • 0x23a7e:$a: NanoCore • 0x29262:$a: NanoCore • 0x292ac:$a: NanoCore • 0x29496:$a: NanoCore • 0x239d1:$b: ClientPlugin • 0x23a0e:$b: ClientPlugin • 0x2430c:$b: ClientPlugin • 0x24319:$b: ClientPlugin • 0x28ffb:$b: ClientPlugin • 0x2926b:$b: ClientPlugin • 0x292b5:$b: ClientPlugin • 0x297cd:$c: ProjectData • 0x19137:$e: KeepAlive • 0x23e59:$g: LogClientMessage • 0x296c0:$g: LogClientMessage • 0x23dd9:$i: get_Connected • 0x19227:$j: #=q • 0x19257:$j: #=q
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.c3yBu1IF57.exe.39bed06.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4083:$x1: NanoCore.ClientPluginHost
5.2.c3yBu1IF57.exe.39bed06.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4083:$x2: NanoCore.ClientPluginHost • 0x4161:$s4: PipeCreated • 0x409d:$s5: IClientLoggingHost
5.2.c3yBu1IF57.exe.2993b90.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x42d2:$x1: NanoCore.ClientPluginHost
5.2.c3yBu1IF57.exe.2993b90.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x42d2:$x2: NanoCore.ClientPluginHost • 0x43b0:$s4: PipeCreated • 0x42ec:$s5: IClientLoggingHost
5.2.c3yBu1IF57.exe.39c9579.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 29 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

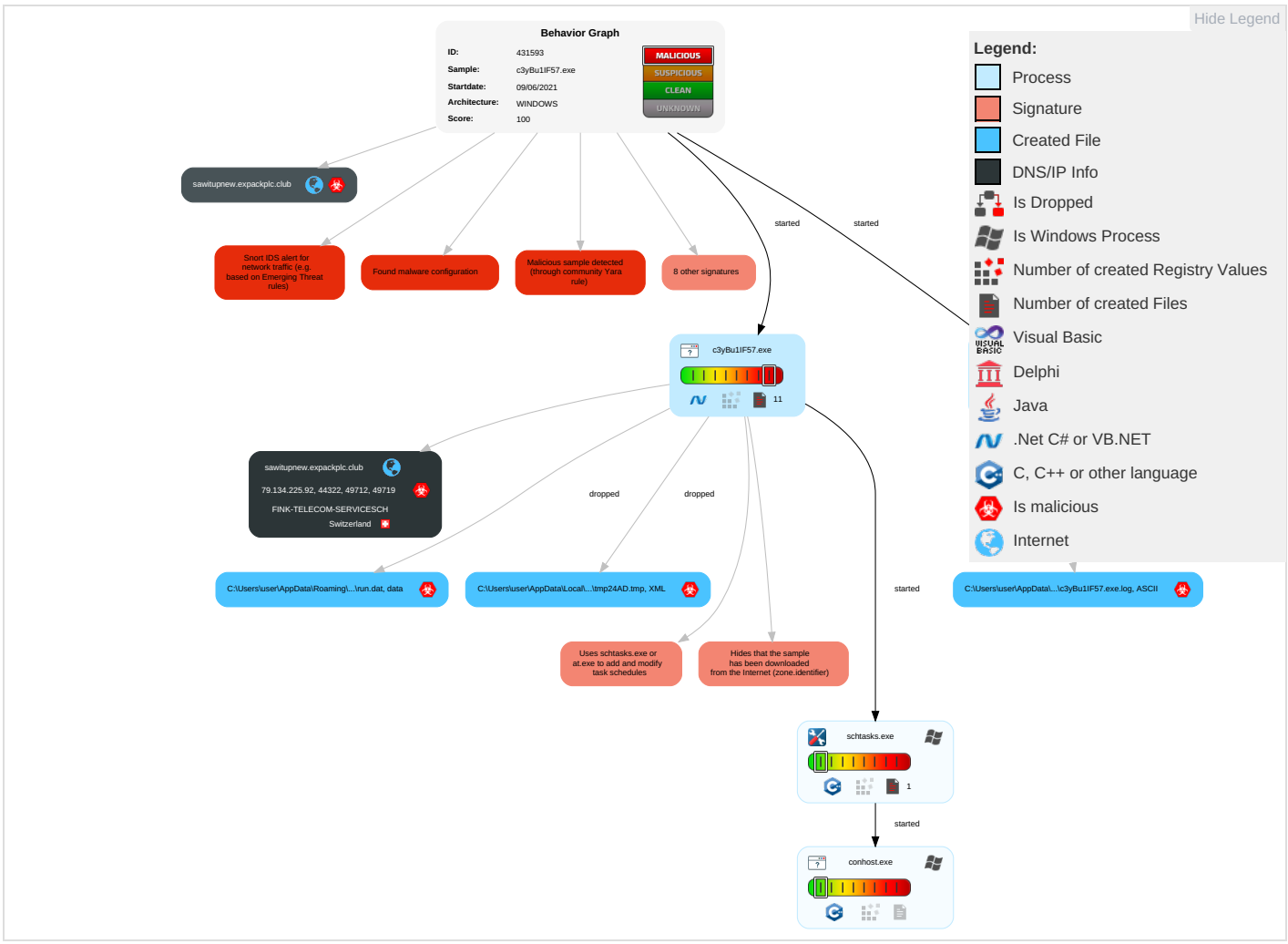
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 1	Input Capture 1 1	Process Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po

Behavior Graph

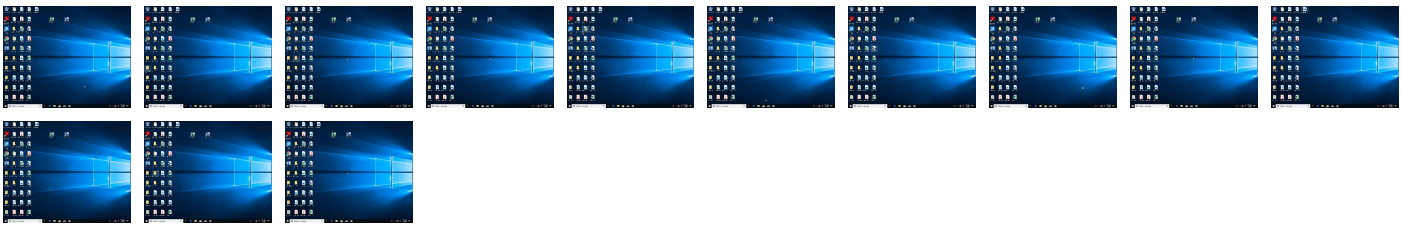
Copyright Joe Security LLC 2021



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
c3yBu1IF57.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
c3yBu1IF57.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
c3yBu1IF57.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.c3yBu1IF57.exe.e20000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.c3yBu1IF57.exe.3b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.c3yBu1IF57.exe.3b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sawitupnew.expackplc.club	79.134.225.92	true	true		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.92	sawitupnew.expackplc.club	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431593
Start date:	09.06.2021
Start time:	00:14:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c3yBu1IF57.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:	28
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@20/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
00:15:10	API Interceptor	1045x Sleep call for process: c3yBu1IF57.exe modified
00:15:11	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\c3yBu1IF57.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.92	l00VLAF9y0xQ9Vr.exe	Get hash	malicious	Browse	
	Gyb49LK8hq.exe	Get hash	malicious	Browse	
	ORDER-210067.xls.exe	Get hash	malicious	Browse	
	n7dlHuG3v6.exe	Get hash	malicious	Browse	
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	
	ORDER-0319.pdf.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.31706.exe	Get hash	malicious	Browse	
	ORDER-21031566AF.exe	Get hash	malicious	Browse	
	10UNv6Ul0W.exe	Get hash	malicious	Browse	
	ORDER-02108 xls.exe	Get hash	malicious	Browse	
	ORDER #0206.exe	Get hash	malicious	Browse	
	ORDER #210 xls.exe	Get hash	malicious	Browse	
	ORDER-2114 doc.exe	Get hash	malicious	Browse	
	INVOICE-0966542R.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	ORDER #0421 pdf.exe	Get hash	malicious	Browse	
	Payment Copy.exe	Get hash	malicious	Browse	
	Pi.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sawitupnew.expackplc.club	l00VLAF9y0xQ9Vr.exe	Get hash	malicious	Browse	• 79.134.225.92

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	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
	A2PlnLyOA7.exe	Get hash	malicious	Browse	• 79.134.225.90
	PDF 209467_9377363745_378341152.exe	Get hash	malicious	Browse	• 79.134.225.11
	v4nJnRl1gt.exe	Get hash	malicious	Browse	• 79.134.225.9
	Invoice#282730.exe	Get hash	malicious	Browse	• 79.134.225.9
	Urban Receipt.exe	Get hash	malicious	Browse	• 79.134.225.9

Copyright Joe Security LLC 2021

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\c3yBu1IF57.exe.log	
Process:	C:\Users\user\Desktop\c3yBu1IF57.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp24AD.tmp	
Process:	C:\Users\user\Desktop\c3yBu1IF57.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.1223050895148425
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Naxtn:cbk4oL600QydbQxIYODOLedq3zj
MD5:	3497D83793A24831446ADB5229803ACB
SHA1:	92D84903CE397DEBB29CB41E1D85B01016664C1E
SHA-256:	9C2CD2A62649CA1506354C439137A0BD9FA28521FD9786EF786CECB84BE72ED5
SHA-512:	43D70CB9DB623E59A29045248C516D267979B9C0EE955D08CDDB8A4BDA9E2DD2C02B890C9D53C62D5B5B8E0648D6C521041E253074769D23D73F402851C70B
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\c3yBu1IF57.exe
File Type:	data
Category:	dropped
Size (bytes):	2728
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	48:Ik/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH87:ft3Ucrt3Ucrt3Ucrt3Ucrt3Ucrt3UcrN
MD5:	3F16EC9869DEDFFEC07792CA71B87AB5
SHA1:	124F3AAEB04E11DEA7361736CE472750D237D3D2
SHA-256:	1A187F3EF38284FF4EE2B20D6021C884E42FC72284F2DA858D7E389CE9C7D0E9
SHA-512:	8DDE0277C2F8CF1CEF64B1EDF120C4A239619FBE9513C833C94B9A429984ECB8AD2A346FD9E333270207951021CCB0CA08FFCDF2ADE538AAFC2B5FAAA1ADF 0A2

<table>
<tr><th colspan="2">C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat</th></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz....''....r...w&&|..c..3}~.....~...os..f.......4..1 .gJ.'.d''.L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz....''... .r...w&&|..c..3}~.....~...os..f.......4..1.gJ.'.d''.L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz....''....r...w&&|..c..3}~.....~...os..f.......4..1.gJ.'.d''.L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B... ....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz....''....r...w&&|..c..3}~.....~...os..f.......4..1.gJ.'.d''.L...A.t...F.{....C.|&.wGj.h\.3.</td></tr>
</table>

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\c3yBu1IF57.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:FmF:IF
MD5:	2758CC201B8FC3F181975D9C7FD76AF8
SHA1:	72156F42778929C21864DBC28642B55094F05DF8
SHA-256:	1D93C878DCE046A43BE9BB33B734C47E3EB28BC3A068A4C418D182ACF9CA17C7
SHA-512:	4F7BA4F6C79125E48826696616B34BD342E43350DCD5A9BA7DF8460C8E7E9BDB83481A16E3CEFBAB69E762EFD684BC71137DBE3AE849D43E46F10F59467EDEB6
Malicious:	**true**
Reputation:	low
Preview:	6..P.+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\c3yBu1IF57.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.5944564061110205
Encrypted:	false
SSDEEP:	3:oNWXp5vGDBsAC:oNWXpFGGAC
MD5:	B4549BC5ECDA1FE84F136E4F546A84E2
SHA1:	6EEBA80994809E878052728063201704584O3EA3
SHA-256:	3894566F927E085853A06BAB39B68A050C3CFD164E1C13267F1EBABE040536F4
SHA-512:	68548AC66042C49BB52921392520172A043F86D2CC9D0C8A497D951BFFDE78B3076EE25BFB69C2ECD877B09F24448E34F8082E5F8F222D809854A77D834D36EB
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\c3yBu1IF57.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.476735179147602
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:	c3yBu1IF57.exe
File size:	215040
MD5:	04f4a27d282ec9ea66549f35b6ff0559
SHA1:	8b8f849c58baa0b439c74310986d6702e45ea118
SHA256:	4da007eb010d6b86861eced1f00ec48423dedc7aec6b0f7942e668c16ebe82d3

Copyright Joe Security LLC 2021

General

SHA512:	6365c4d2b7da6468dbc524d5ac6703c61c8d70fe30fdd1dc432cd6dae71f48f921e13154d159594d6e5e327fc68709732cad35a626a1584677bcec676a10a969
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HI/HAeptZlcVzYSU+bE12N93Kv:gLV6Bta6dtJmaklM5/ep3lSzV57fK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....~..... .....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
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:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0x1c798	0x1c800	False	0.594512404057	data	6.5980802599	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x17a98	0x17c00	False	0.997152549342	data	7.99762154799	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-00:15:11.597880	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:18.008471	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:24.952094	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:31.813106	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:38.228294	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:44.621663	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:51.058775	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	44322	192.168.2.3	79.134.225.92
06/09/21-00:15:56.135293	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:03.688404	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:10.109966	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:17.616791	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:23.859860	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:30.211817	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:36.435451	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:42.677464	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:48.996299	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:53.788174	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	44322	192.168.2.3	79.134.225.92
06/09/21-00:16:59.940102	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	44322	192.168.2.3	79.134.225.92
06/09/21-00:17:06.143024	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	44322	192.168.2.3	79.134.225.92
06/09/21-00:17:12.310339	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	44322	192.168.2.3	79.134.225.92

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 00:15:11.246614933 CEST	192.168.2.3	8.8.8.8	0xec49	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:17.691190958 CEST	192.168.2.3	8.8.8.8	0x1a2d	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:24.650753975 CEST	192.168.2.3	8.8.8.8	0x8ae4	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:31.516273975 CEST	192.168.2.3	8.8.8.8	0x52c3	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:37.908292055 CEST	192.168.2.3	8.8.8.8	0x2134	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:44.292639971 CEST	192.168.2.3	8.8.8.8	0x32ca	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:50.761687994 CEST	192.168.2.3	8.8.8.8	0x2877	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:55.837618113 CEST	192.168.2.3	8.8.8.8	0x1fe7	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:03.390366077 CEST	192.168.2.3	8.8.8.8	0xfc7a	Standard query (0)	sawitupnew.expackplc.club	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 00:16:09.809451103 CEST	192.168.2.3	8.8.8.8	0x93e6	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:17.290998936 CEST	192.168.2.3	8.8.8.8	0x391c	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:23.543833971 CEST	192.168.2.3	8.8.8.8	0xc552	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:29.900594950 CEST	192.168.2.3	8.8.8.8	0x1174	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:36.141757011 CEST	192.168.2.3	8.8.8.8	0xc8ce	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:42.384780884 CEST	192.168.2.3	8.8.8.8	0x88da	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:48.694340944 CEST	192.168.2.3	8.8.8.8	0xdff8	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:53.488142967 CEST	192.168.2.3	8.8.8.8	0x280e	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:59.643735886 CEST	192.168.2.3	8.8.8.8	0x5846	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:17:05.843000889 CEST	192.168.2.3	8.8.8.8	0x6d15	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)
Jun 9, 2021 00:17:12.014848948 CEST	192.168.2.3	8.8.8.8	0xfc9	Standard query (0)	sawitupnew .expackplc.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 00:15:11.296870947 CEST	8.8.8.8	192.168.2.3	0xec49	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:17.739301920 CEST	8.8.8.8	192.168.2.3	0x1a2d	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:24.695622921 CEST	8.8.8.8	192.168.2.3	0x8ae4	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:31.564423084 CEST	8.8.8.8	192.168.2.3	0x52c3	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:37.957299948 CEST	8.8.8.8	192.168.2.3	0x2134	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:44.371109009 CEST	8.8.8.8	192.168.2.3	0x32ca	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:50.810390949 CEST	8.8.8.8	192.168.2.3	0x2877	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:15:55.882657051 CEST	8.8.8.8	192.168.2.3	0x1fe7	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:03.436137915 CEST	8.8.8.8	192.168.2.3	0xfc7a	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:09.855406046 CEST	8.8.8.8	192.168.2.3	0x93e6	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:17.333616972 CEST	8.8.8.8	192.168.2.3	0x391c	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:23.589648962 CEST	8.8.8.8	192.168.2.3	0xc552	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:29.952039003 CEST	8.8.8.8	192.168.2.3	0x1174	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:36.184793949 CEST	8.8.8.8	192.168.2.3	0xc8ce	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:42.427835941 CEST	8.8.8.8	192.168.2.3	0x88da	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:48.740958929 CEST	8.8.8.8	192.168.2.3	0xdff8	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:16:53.533478022 CEST	8.8.8.8	192.168.2.3	0x280e	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 00:16:59.687155962 CEST	8.8.8.8	192.168.2.3	0x5846	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:17:05.887877941 CEST	8.8.8.8	192.168.2.3	0x6d15	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)
Jun 9, 2021 00:17:12.059387922 CEST	8.8.8.8	192.168.2.3	0xfc9	No error (0)	sawitupnew .expackplc.club		79.134.225.92	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: c3yBu1IF57.exe PID: 5564 Parent PID: 5764

General

Start time:	00:15:08
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\c3yBu1IF57.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\c3yBu1IF57.exe'
Imagebase:	0xe20000
File size:	215040 bytes
MD5 hash:	04F4A27D282EC9EA66549F35B6FF0559
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: 00000000.00000000.198137342.0000000000E22000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.198137342.0000000000E22000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.198137342.0000000000E22000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5408 Parent PID: 5564

General

Start time:	00:15:09
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp24AD.tmp'
Imagebase:	0x13e0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1240 Parent PID: 5408

General

Start time:	00:15:09
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: c3yBu1IF57.exe PID: 6080 Parent PID: 528

General

Start time:	00:15:11
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\c3yBu1IF57.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\c3yBu1IF57.exe 0
Imagebase:	0x3b0000
File size:	215040 bytes
MD5 hash:	04F4A27D282EC9EA66549F35B6FF0559
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.204561377.00000000003B2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.204561377.00000000003B2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.204561377.00000000003B2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.219125636.0000000002971000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.219125636.0000000002971000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.218347398.00000000003B2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.218347398.00000000003B2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.218347398.00000000003B2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.219165813.0000000003971000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.219165813.0000000003971000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021