ID: 402647
Sample Name:
b2NaDSFu9T.exe
Cookbook: default.jbs
Time: 11:34:42
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

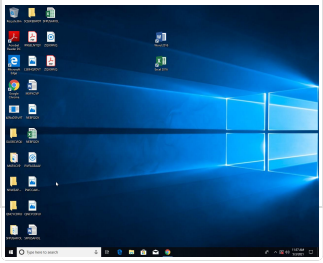
Analysis Report b2NaDSFu9T.exe

Overview

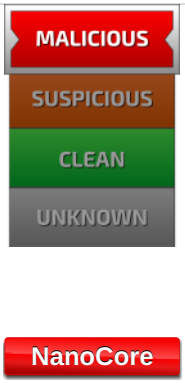
General Information

Sample Name:	b2NaDSFu9T.exe
Analysis ID:	402647
MD5:	042aa11c6d49e1..
SHA1:	5a89ff2f9702a53…
SHA256:	3383218b916baf1.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



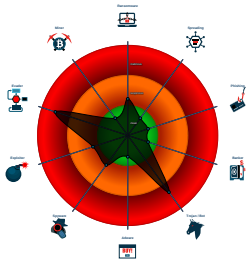
NanoCore

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

Signatures

- 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 AntiVM3
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- b2NaDSFu9T.exe (PID: 5340 cmdline: 'C:\Users\user\Desktop\b2NaDSFu9T.exe' MD5: 042AA11C6D49E1CCA5923F02D1B0A5AE)
  - RegSvcs.exe (PID: 4892 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": ".0.0.0,",
  "Mutex": "21f4355e-8257-4e77-8f1b-c822c6ea",
  "Group": "BUILD",
  "Domain1": "79.134.225.26",
  "Domain2": "nassiru1166main.ddns.net",
  "Port": 1133,
  "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"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.258945318.0000000002F4B000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.260256472.0000000003F11000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2a02ad:$x1: NanoCore.ClientPluginHost • 0x3252cd:$x1: NanoCore.ClientPluginHost • 0x2a02ea:$x2: IClientNetworkHost • 0x32530a:$x2: IClientNetworkHost • 0x2a3e1d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x328e3d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.260256472.0000000003F11000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.260256472.0000000003F11000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2a0015:$a: NanoCore • 0x2a0025:$a: NanoCore • 0x2a0259:$a: NanoCore • 0x2a026d:$a: NanoCore • 0x2a02ad:$a: NanoCore • 0x325035:$a: NanoCore • 0x325045:$a: NanoCore • 0x325279:$a: NanoCore • 0x32528d:$a: NanoCore • 0x3252cd:$a: NanoCore • 0x2a0074:$b: ClientPlugin • 0x2a0276:$b: ClientPlugin • 0x2a02b6:$b: ClientPlugin • 0x325094:$b: ClientPlugin • 0x325296:$b: ClientPlugin • 0x3252d6:$b: ClientPlugin • 0x2a019b:$c: ProjectData • 0x3251bb:$c: ProjectData • 0x2a0ba2:$d: DESCrypto • 0x325bc2:$d: DESCrypto • 0x2a856e:$e: KeepAlive
Process Memory Space: b2NaDSFu9T.exe PID: 5340	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.b2NaDSFu9T.exe.41a1120.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x951ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x951ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x98d1d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.b2NaDSFu9T.exe.41a1120.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.b2NaDSFu9T.exe.41a1120.2.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x94f15:$a: NanoCore • 0x94f25:$a: NanoCore • 0x95159:$a: NanoCore • 0x9516d:$a: NanoCore • 0x951ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x94f74:$b: ClientPlugin • 0x95176:$b: ClientPlugin • 0x951b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x9509b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x95aa2:$d: DESCrypto • 0x1844e:$e: KeepAlive
0.2.b2NaDSFu9T.exe.41a1120.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

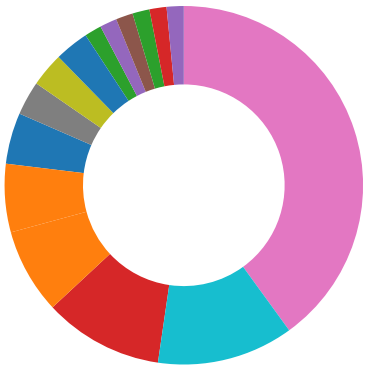
Source	Rule	Description	Author	Strings
0.2.b2NaDSFu9T.exe.41a1120.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
Click to see the 2 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

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)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

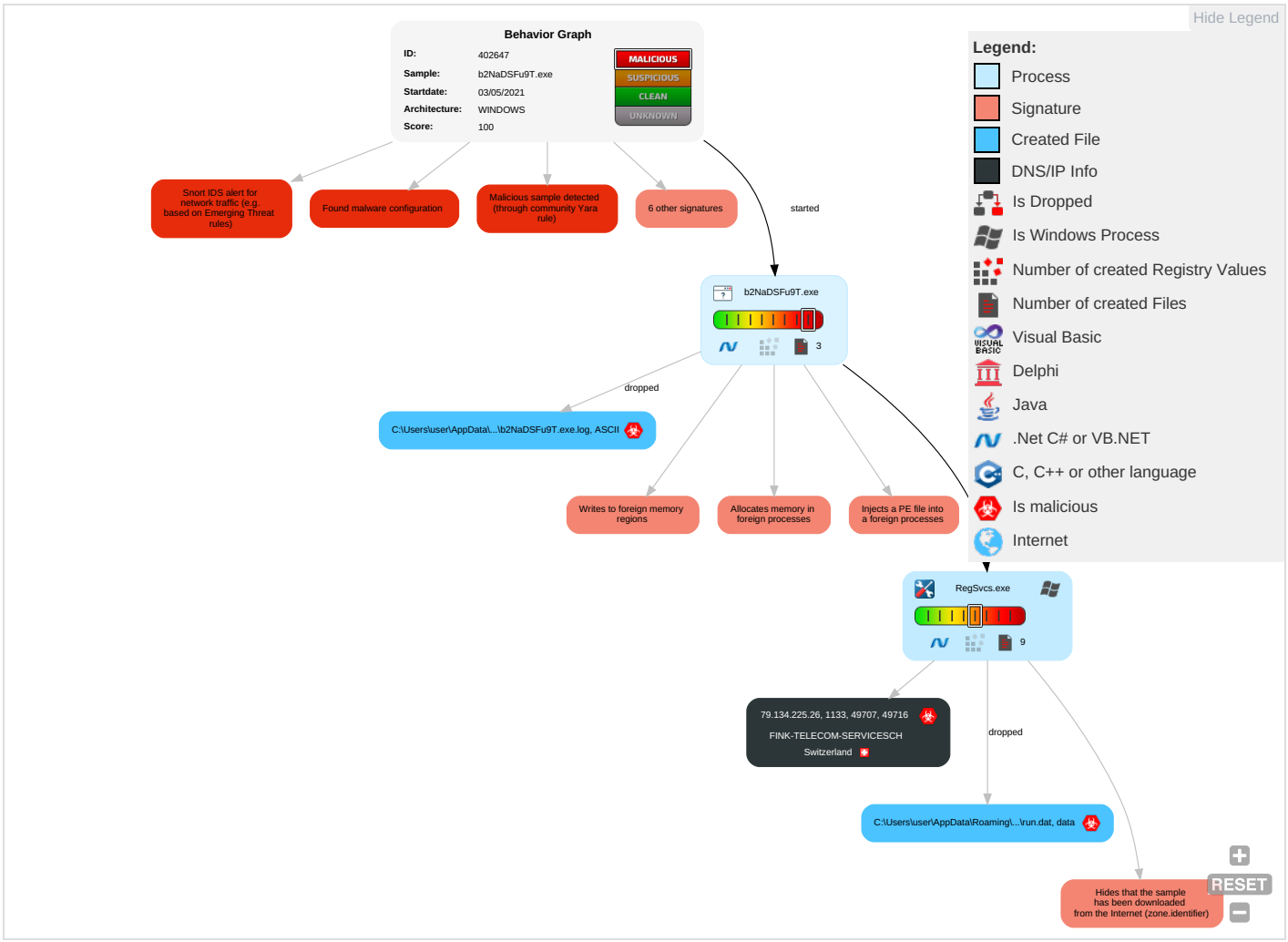
Remote Access Functionality:

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	Windows Management Instrumentation	Path Interception	Process Injection 3 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po

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
b2NaDSFu9T.exe	18%	Virustotal		Browse
b2NaDSFu9T.exe	17%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
79.134.225.26	0%	Avira URL Cloud	safe	
nassiru1166main.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

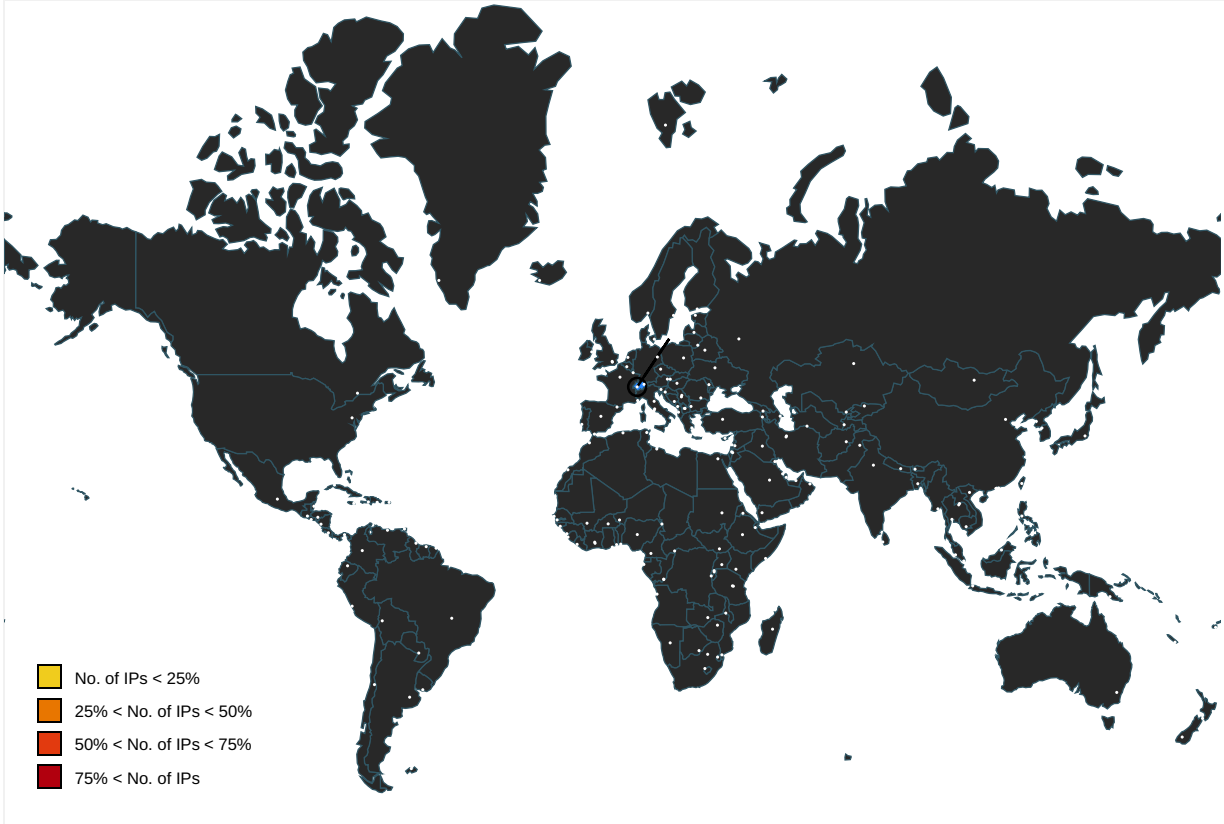
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.26	true	• Avira URL Cloud: safe	unknown
nassiru1166main.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/unguest	b2NaDSFu9T.exe	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	b2NaDSFu9T.exe, 00000000.00000002.258945318.0000000002F4B000.00000004.00000001.sdmp	false		high
http://https://github.com/unguest9WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionGProperty	b2NaDSFu9T.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.26	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402647
Start date:	03.05.2021
Start time:	11:34:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	b2NaDSFu9T.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:	26
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@3/3@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.3%) • Quality average: 77% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 82% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
11:35:53	API Interceptor	1x Sleep call for process: b2NaDSFu9T.exe modified
11:35:55	API Interceptor	1060x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.26	Original title deed.xlsx	Get hash	malicious	Browse	
	PpkzTxJVyC.exe	Get hash	malicious	Browse	
	Original title deed.xlsx	Get hash	malicious	Browse	
	jk55xlWn7a.exe	Get hash	malicious	Browse	
	Qds5xiJaAX.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INVOICE.xlsx	Get hash	malicious	Browse	
	owrCPP2YTC.exe	Get hash	malicious	Browse	
	reorder17032021.PDF.exe	Get hash	malicious	Browse	
	re-order15032021.PDF.exe	Get hash	malicious	Browse	
	new order15032021.PDF.exe	Get hash	malicious	Browse	
	CLEW enquiry 2021.PDF.exe	Get hash	malicious	Browse	
	payment proof.png.exe	Get hash	malicious	Browse	
	0001.exe	Get hash	malicious	Browse	
	Purchase Order 2021-311743-045.xls.exe	Get hash	malicious	Browse	
	CLEW enquiry 2021.PDF.exe	Get hash	malicious	Browse	
	Purchase.exe	Get hash	malicious	Browse	
	Quote.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	invoicedHusrLjViL.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.jc.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 79.134.225.52
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 79.134.225.25
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 79.134.225.25
	SCAN_ORDER & SAMPLES.exe	Get hash	malicious	Browse	• 79.134.225.52
	Apr-advance payment #5972939.exe	Get hash	malicious	Browse	• 79.134.225.9
	PpkzTxJVyC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	jk55xlWn7a.exe	Get hash	malicious	Browse	• 79.134.225.26
	Qds5xiJaAX.exe	Get hash	malicious	Browse	• 79.134.225.26
	INVOICE.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	• 79.134.225.91
	Payment-Confirmation_Copy.exe	Get hash	malicious	Browse	• 79.134.225.108
	owrCPP2YTC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Payment Advice-BCS_ECS9522020090915390034_3159_952.jar	Get hash	malicious	Browse	• 79.134.225.59
	nciv84yXK1.exe	Get hash	malicious	Browse	• 79.134.225.7
	Rechnung.exe	Get hash	malicious	Browse	• 79.134.225.39
	ENrYP02wGO.exe	Get hash	malicious	Browse	• 79.134.225.91

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\b2NaDSFu9T.exe.log

Process:	C:\Users\user\Desktop\b2NaDSFu9T.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\b2NaDSFu9T.exe.log	
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, 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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.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\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	12:X4LEnybgCF7wHJyCe8O6LEnybgCF7wHJyCe8Oh:IQnybgCyHJ5lQnybgCyHJ5i
MD5:	9D28662484E30E8B7C123705C7B0C8E6
SHA1:	BFB9A9E2BDC178B5E8FE1CDFB68D65D8D7F4840A
SHA-256:	F699DB97FD0C37997AA67809552C1B2C6500E07660D0540055896615F12A90D7
SHA-512:	58303088530E6548BBFB1800A52221CE5A29E33A48442DD16524EB1021850E902C0E01FE9035CC8C794E966AFD6A7FA950974E3F1B320A8F37F6090C6D7D3820
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL|X

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:cmr8tn:cNtn
MD5:	0DC2073C953398D28C9D8E44EEA5ADA1
SHA1:	FA0FA923069FACF1AF850D9672C0FC451328C71E
SHA-256:	7376B029584CD7CC2E8EB49E35D9243124AFA2AC557B6141C94788BADD19002A
SHA-512:	83053423035A70D10B0FD614E2267EBE4E6995920E0CF5439CF42E4CFFFB201E3C89E2BFCB9608B0BB9D12B813B0BB0ADC2EBB6A989E2394C7AE162044D84951
Malicious:	**true**
Reputation:	low
Preview:	...lb..H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.956232639570589

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	b2NaDSFu9T.exe
File size:	1141760
MD5:	042aa11c6d49e1cca5923f02d1b0a5ae
SHA1:	5a89ff2f9702a53fb638b8c7229ba868aaa58ae9
SHA256:	3383218b916baf1a46989c4f253b29eb81e97ac763ab716 15c81d85a18495f34
SHA512:	6d0551584f1f4c5391012111be3bc251026d3db6a531ab7 a8ce0d41cf278a254bc8a0bc66690a1a93c3bf52c2c1c70 e7fcd94e4b8812bcea95efa8bda86d7184
SSDEEP:	24576:jVdlEYuS48YvtC/X4kRxlhtJftkKrEMAtugu+/a:jEj X48uAzJEMZry
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..X.....w... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x517792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608FA4A3 [Mon May 3 07:22:11 2021 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x117740	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x118000	0xed0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x11a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x115798	0x115800	False	0.960257425394	data	7.96059480846	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x118000	0xed0	0x1000	False	0.3740234375	data	4.74787952307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x118090	0x3a4	data		
RT_MANIFEST	0x118444	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	InterfaceTypeAttribute.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	InterfaceTypeAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-11:35:57.731947	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:04.057658	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:10.300646	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:16.535954	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:32.356162	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:38.604791	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:44.807678	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:51.125432	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	1133	192.168.2.7	79.134.225.26
05/03/21-11:36:57.381214	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:03.896572	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:13.224491	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:19.689841	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:29.259378	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:35.503934	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:41.765593	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:48.076433	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	1133	192.168.2.7	79.134.225.26
05/03/21-11:37:54.385213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	1133	192.168.2.7	79.134.225.26
05/03/21-11:38:00.574763	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	1133	192.168.2.7	79.134.225.26

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 11:35:57.175148964 CEST	49707	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:35:57.595338106 CEST	1133	49707	79.134.225.26	192.168.2.7
May 3, 2021 11:35:57.595468044 CEST	49707	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:35:57.731946945 CEST	49707	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:35:58.683852911 CEST	49707	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:35:59.095221043 CEST	1133	49707	79.134.225.26	192.168.2.7
May 3, 2021 11:35:59.095515966 CEST	49707	1133	192.168.2.7	79.134.225.26

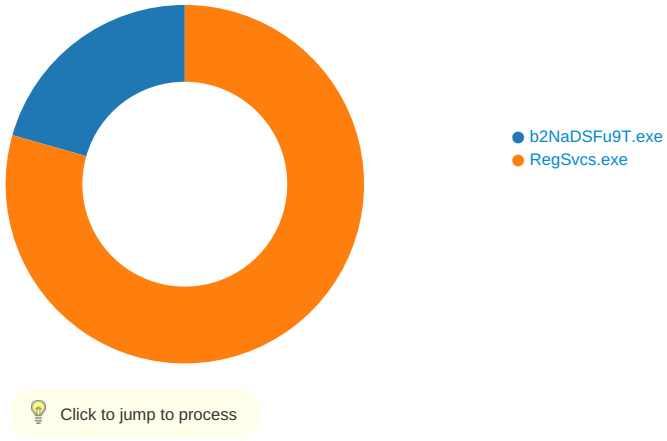
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 11:35:59.475019932 CEST	1133	49707	79.134.225.26	192.168.2.7
May 3, 2021 11:35:59.625859976 CEST	49707	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:35:59.975164890 CEST	1133	49707	79.134.225.26	192.168.2.7
May 3, 2021 11:35:59.975369930 CEST	49707	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:03.701108932 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:04.056865931 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:04.056981087 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:04.057657957 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:04.483517885 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:04.483618975 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:04.535276890 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:04.535418987 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:04.915105104 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:04.915201902 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:05.275497913 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:05.277007103 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:05.735222101 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:05.735450983 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:05.873095989 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:06.155128956 CEST	1133	49716	79.134.225.26	192.168.2.7
May 3, 2021 11:36:06.155272961 CEST	49716	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:09.895852089 CEST	49721	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:10.295373917 CEST	1133	49721	79.134.225.26	192.168.2.7
May 3, 2021 11:36:10.295598984 CEST	49721	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:10.300646067 CEST	49721	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:11.184920073 CEST	49721	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:12.092092037 CEST	49721	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:12.483063936 CEST	1133	49721	79.134.225.26	192.168.2.7
May 3, 2021 11:36:12.483128071 CEST	49721	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:16.109191895 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:16.535310984 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:16.535440922 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:16.535953999 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:16.975370884 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:16.975955009 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:17.075939894 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:17.076164007 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:17.455312014 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:17.458092928 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:17.564977884 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:17.565160036 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:17.863342047 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:17.864617109 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:18.236253977 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:18.483088017 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:18.835776091 CEST	1133	49724	79.134.225.26	192.168.2.7
May 3, 2021 11:36:18.835900068 CEST	49724	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:22.543319941 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:22.895484924 CEST	1133	49725	79.134.225.26	192.168.2.7
May 3, 2021 11:36:22.895659924 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:23.134715080 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:23.857887030 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:24.216471910 CEST	1133	49725	79.134.225.26	192.168.2.7
May 3, 2021 11:36:24.216588974 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:24.623435974 CEST	1133	49725	79.134.225.26	192.168.2.7
May 3, 2021 11:36:24.936151028 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:24.936708927 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:25.323057890 CEST	1133	49725	79.134.225.26	192.168.2.7
May 3, 2021 11:36:25.324203014 CEST	49725	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:28.954962015 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:31.967937946 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:32.355309963 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:32.355513096 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:32.356162071 CEST	49728	1133	192.168.2.7	79.134.225.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 11:36:32.755695105 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:32.755803108 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:32.935302019 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:32.936120033 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:33.225116968 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:33.227468014 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:33.355937958 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:33.358747959 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:33.776004076 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:34.218465090 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:34.623622894 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:34.623821020 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:37.735433102 CEST	1133	49728	79.134.225.26	192.168.2.7
May 3, 2021 11:36:37.735807896 CEST	49728	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:38.235639095 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:38.603579044 CEST	1133	49729	79.134.225.26	192.168.2.7
May 3, 2021 11:36:38.603712082 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:38.604790926 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:39.037123919 CEST	1133	49729	79.134.225.26	192.168.2.7
May 3, 2021 11:36:39.037262917 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:39.178581953 CEST	1133	49729	79.134.225.26	192.168.2.7
May 3, 2021 11:36:39.178910017 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:39.562207937 CEST	1133	49729	79.134.225.26	192.168.2.7
May 3, 2021 11:36:39.796814919 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:40.223459959 CEST	1133	49729	79.134.225.26	192.168.2.7
May 3, 2021 11:36:40.422703028 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:40.819509983 CEST	1133	49729	79.134.225.26	192.168.2.7
May 3, 2021 11:36:40.819602966 CEST	49729	1133	192.168.2.7	79.134.225.26
May 3, 2021 11:36:44.439085960 CEST	49730	1133	192.168.2.7	79.134.225.26

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: b2NaDSFu9T.exe PID: 5340 Parent PID: 5620

General

Start time:	11:35:52
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\b2NaDSFu9T.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\b2NaDSFu9T.exe'
Imagebase:	0x7c0000
File size:	1141760 bytes
MD5 hash:	042AA11C6D49E1CCA5923F02D1B0A5AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.258945318.0000000002F4B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.260256472.0000000003F11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.260256472.0000000003F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.260256472.0000000003F11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\b2NaDSFu9T.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\b2NaDSFu9T.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7273A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile

Analysis Process: RegSvcs.exe PID: 4892 Parent PID: 5340

General

Start time:	11:35:54
Start date:	03/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x750000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	50D07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	50D089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	50D07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	50D07A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	7	50D089B	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	14 01 da 49 62 0e d9 48	...Ib..H	success or wait	1	50D0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	216	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 50 f4 76 59 a1 02 b3 8b 02 19 e1 11 b5 53 f0 35 8a 36 12 43 34 2e dd 45 b1 59 db 7c f7 f1 8d 15 ba ff 7f 82 16 29 8e 7a 73 0c a9 ef 77 e2 b4 67 6c ef e7 5c ec 47 c3 1a 4a 18 4d f2 76 45 53 8c 30 e0 df 9b ff d2 9b 50 f7 3a 82 b9 36 fc f0 01 54 a7 89 a5 c8 2b 35 80 31 a7 c4 19 c1 b3 0c ea a6 a9 b1 9d e7 e0 c5 72 06 50 1d 56 9b 95 2b 91 e6 28 cc 2a 32 64 09 66 87 b6 cf 20 ed ed ba 9e 71 c3 85 cb 20 37 69 4f ca 2b 81 bb 63 da e6 8b b2 fa cf 09 21 c9 27 ed 2a c7 14 6d 4c 7c 58	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h.P.v Y.....S.5.6.C4..E.Y.|..... ....).zs...w..gl..\.G..J.M.vES .0.....P.:...6...T....+5.1.... .....r.P.V..+..(.*2d.f... ....q... 7iO.+..c.....!.'.* ..mL|X	success or wait	2	50D0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	50D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	50D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	50D0A53	ReadFile

Disassembly

Code Analysis