ID: 432605
Sample Name: dYy3yfSkwY.exe
Cookbook: default.jbs
Time: 15:30:25
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

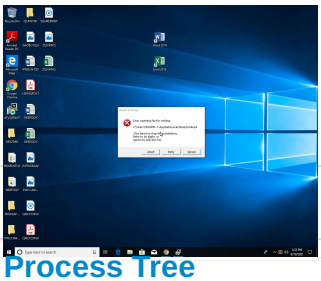
Analysis Report dYy3yfSkwY.exe

Overview

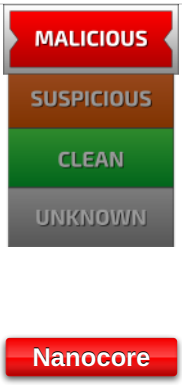
General Information

Sample Name:	dYy3yfSkwY.exe
Analysis ID:	432605
MD5:	3deb8b7e51c21c..
SHA1:	f98809b1b883912.
SHA256:	c0503f7c65391a5..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



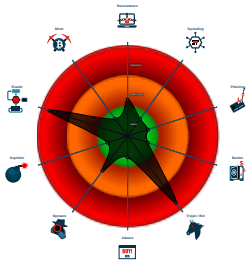
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- 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…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- dYy3yfSkwY.exe (PID: 6108 cmdline: 'C:\Users\user\Desktop\dYy3yfSkwY.exe' MD5: 3DEB8B7E51C21CBA0C2C723C5AF953DD)
  - dYy3yfSkwY.exe (PID: 668 cmdline: 'C:\Users\user\Desktop\dYy3yfSkwY.exe' MD5: 3DEB8B7E51C21CBA0C2C723C5AF953DD)
- opjlpsercy.exe (PID: 3724 cmdline: 'C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe' MD5: 3DEB8B7E51C21CBA0C2C723C5AF953DD)
  - opjlpsercy.exe (PID: 4520 cmdline: 'C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe' MD5: 3DEB8B7E51C21CBA0C2C723C5AF953DD)
- opjlpsercy.exe (PID: 5892 cmdline: 'C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe' MD5: 3DEB8B7E51C21CBA0C2C723C5AF953DD)
- **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

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.317958007.000000000400000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x251e5:$x1: NanoCore.ClientPluginHost • 0x25222:$x2: IClientNetworkHost • 0x28d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000002.317958007.000000000400000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.317958007.000000000400000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x24f4d:$a: NanoCore • 0x24f5d:$a: NanoCore • 0x25191:$a: NanoCore • 0x251a5:$a: NanoCore • 0x251e5:$a: NanoCore • 0x24fac:$b: ClientPlugin • 0x251ae:$b: ClientPlugin • 0x251ee:$b: ClientPlugin • 0x250d3:$c: ProjectData • 0x25ada:$d: DESCrypto • 0x2d4a6:$e: KeepAlive • 0x2b494:$g: LogClientMessage • 0x2768f:$i: get_Connected • 0x25e10:$j: #=q • 0x25e40:$j: #=q • 0x25e5c:$j: #=q • 0x25e8c:$j: #=q • 0x25ea8:$j: #=q • 0x25ec4:$j: #=q • 0x25ef4:$j: #=q • 0x25f10:$j: #=q
0000000B.00000002.319773965.000000000396D000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.319773965.000000000396D000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x139f05:$a: NanoCore • 0x139f5e:$a: NanoCore • 0x139f9b:$a: NanoCore • 0x13a014:$a: NanoCore • 0x142ae8:$a: NanoCore • 0x142b0d:$a: NanoCore • 0x142b66:$a: NanoCore • 0x152d03:$a: NanoCore • 0x152d29:$a: NanoCore • 0x152d85:$a: NanoCore • 0x15fbda:$a: NanoCore • 0x15fc33:$a: NanoCore • 0x15fc66:$a: NanoCore • 0x15fe92:$a: NanoCore • 0x15ff0e:$a: NanoCore • 0x160527:$a: NanoCore • 0x160670:$a: NanoCore • 0x160b44:$a: NanoCore • 0x160e2b:$a: NanoCore • 0x160e42:$a: NanoCore • 0x1663e0:$a: NanoCore
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.opjlpsercy.exe.3ab7184.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
11.2.opjlpsercy.exe.3ab7184.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
11.2.opjlpsercy.exe.290b950.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
11.2.opjlpsercy.exe.290b950.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
7.2.opjlpsercy.exe.9810000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 105 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:

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

Compliance:

Detected unpacking (overwrites its own PE header)

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:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

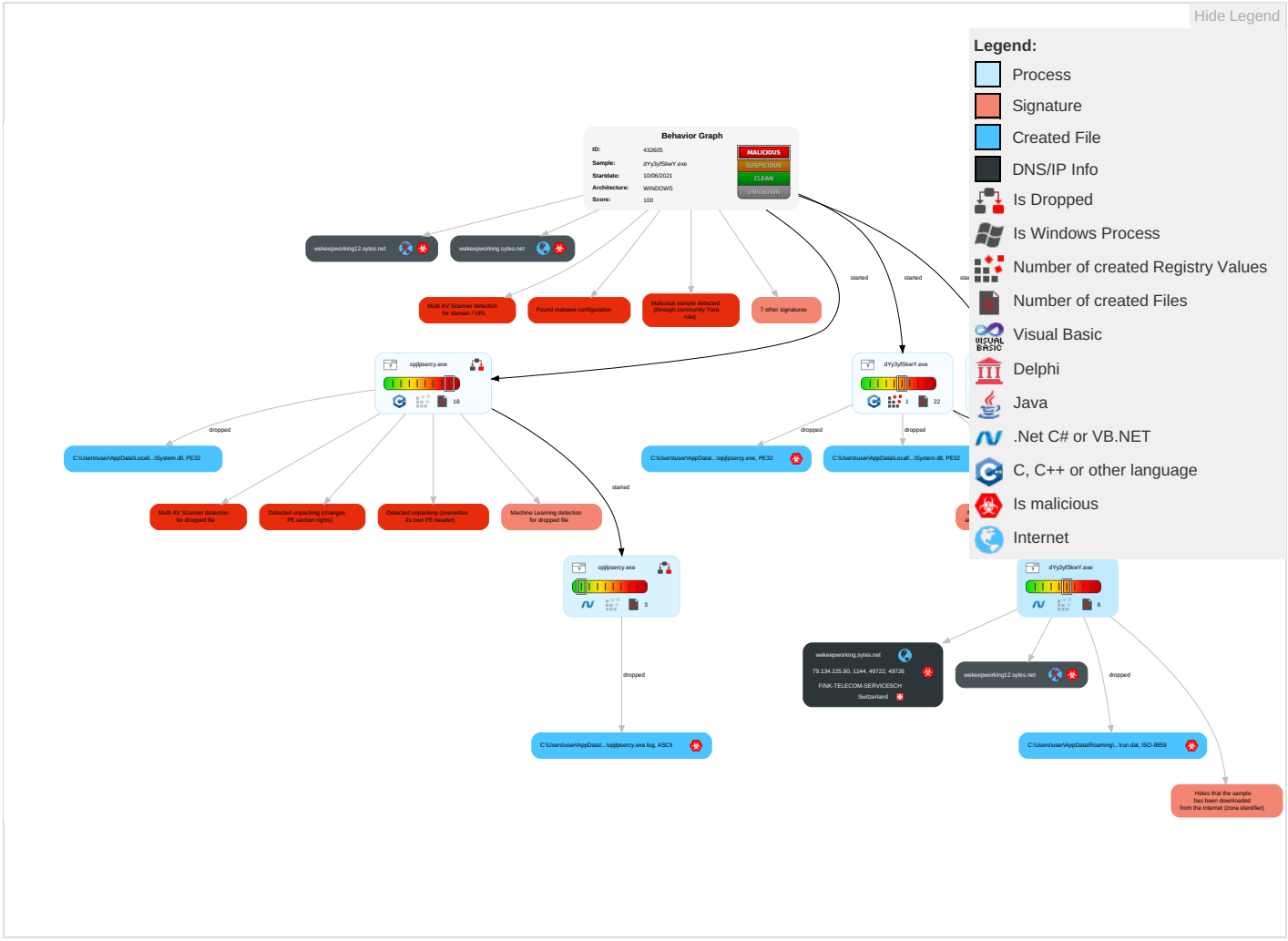
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdı Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 1	NTDS	Security Software Discovery 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	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	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

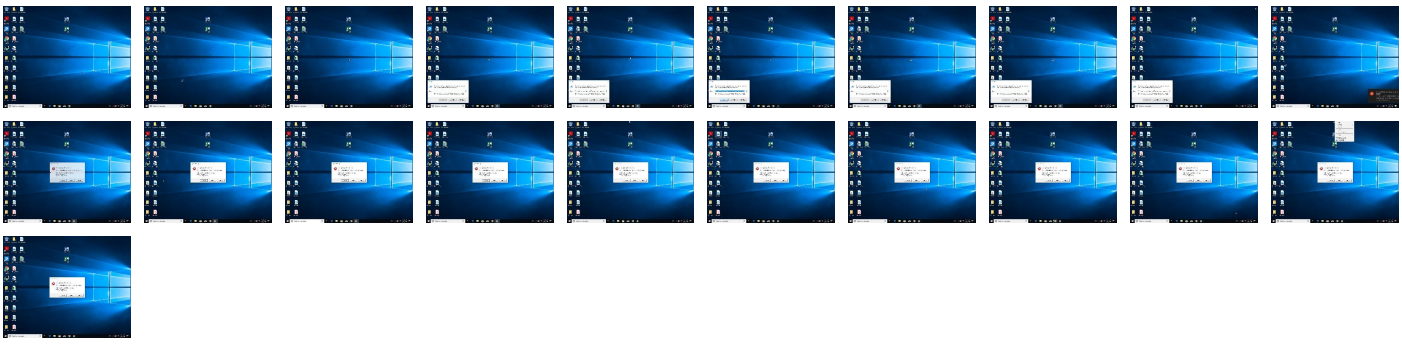
Behavior Graph



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
dYy3yfSkwY.exe	19%	Virustotal		Browse
dYy3yfSkwY.exe	35%	ReversingLabs	Win32.Trojan.NanoBot	
dYy3yfSkwY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nso6CF2.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso6CF2.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz21EF.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsz21EF.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe	35%	ReversingLabs	Win32.Trojan.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.dYy3yfSkwY.exe.9920000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.0.opjlpsercy.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
11.0.opjlpsercy.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
11.2.opjlpsercy.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.dYy3yfSkwY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
14.0.opjlpsercy.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.0.dYy3yfSkwY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
7.2.opjlpsercy.exe.40ff3e.2.unpack	100%	Avira	ADWARE/Patched.Ren.Gen7		Download File
7.2.opjlpsercy.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
11.1.opjlpsercy.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.dYy3yfSkwY.exe.40ff3e.2.unpack	100%	Avira	ADWARE/Patched.Ren.Gen7		Download File
3.1.dYy3yfSkwY.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.opjlpsercy.exe.4b00000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.opjlpsercy.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
3.0.dYy3yfSkwY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		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	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	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

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:	432605
Start date:	10.06.2021

Start time:	15:30:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dYy3yfSkwY.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:	29
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@7/13@58/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 77.4% (good quality ratio 72.2%) • Quality average: 79.4% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 80% • 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
15:31:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ppeejliapu C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
15:31:28	API Interceptor	870x Sleep call for process: dYy3yfSkwY.exe modified
15:31:35	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ppeejliapu C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
15:31:41	API Interceptor	1x Sleep call for process: opjlpsercy.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.90	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	ZVFVY7NwZ7.exe	Get hash	malicious	Browse	
	kylfnzzg3E.exe	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	ZVFVY7NwZ7.exe	Get hash	malicious	Browse	• 79.134.225.90
	kyIfnzzg3E.exe	Get hash	malicious	Browse	• 79.134.225.90
	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
	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	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	ZVFVY7NwZ7.exe	Get hash	malicious	Browse	• 79.134.225.90
	0jyrU2E05S.exe	Get hash	malicious	Browse	• 79.134.225.72
	kyIfnzzg3E.exe	Get hash	malicious	Browse	• 79.134.225.90
	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
	c3yBu1lF57.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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nso6CF2.tmp\System.dll	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	
	PO187439.exe	Get hash	malicious	Browse	
	090009000000090.exe	Get hash	malicious	Browse	
	NEWORDERLIST.exe	Get hash	malicious	Browse	
	00404000004.exe	Get hash	malicious	Browse	
	40900900090000.exe	Get hash	malicious	Browse	
	INVO090090202.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.Injector.AIC.genEldorado.29599.exe	Get hash	malicious	Browse	
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.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\eq64oqvr7vut3n4dt5cu

Process:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
File Type:	data
Category:	modified
Size (bytes):	616448
Entropy (8bit):	**7.999692733314968**
Encrypted:	**true**
SSDEEP:	12288:2Ph/JQuO9xgeB2Q54fr2dM4av0CGBmhFoqS3UDmhcOQV5eZTr:6diuMxgy6frQuv0L0hFoqSkDmhcOsS/
MD5:	7A73EF366D5F76E92D47C3064D0E3A26
SHA1:	C7638BBDAB4934280BD2A5F5B004623568BBD876
SHA-256:	55713D87E066560138EB389AB6FE3DB6EA642EB5C0149992FC99A38D09AA86B4
SHA-512:	908A167E2692BA331A06770A818FA9C2A7CB325374A2EEA086FB499B6069B6B7D0C6667D49BB49DDC5877B8A2BA22ABF9E0AF531A38487058CBBF7408D9C190
Malicious:	false
Reputation:	low
Preview:	}.....e... 6..5Ckz...p.wB....}...e..O./r.5R..r.V..;]A.N..Jgmi...Z%r.R.)4...-4..pYG.q..by.....|.=~_+xi.@N...+<.!.R.m.f~}..!*.(C.....[.4@?1..._.l.5....l.....+..cy..+]...U*.u5...f.}n....t.F.=..$d..D...GX...0H..J6...J.BT..%...O..t.'P....f.....u..._<.f&(Z.K....^..W.?...?..k.k@...z.....O.R..N..Jsl.)i.8n.:...k*..`..]...,3.[j.{UE...>.Q.]J-...(..G~....%p...x...~.Gv.....t.....3..:U3.FG..$rr.).....,....2.!.o.B.....~....'.x...c..V43.....,].0L{.KII0....d0...4.....#..._P.T+..ROQ...3..1.Z...)._*.G,...*...>.`.....c.b]..B.....j....?..+.F..P?.....[p/\u.3..Q.j..d....<+...~S.....t..:=Z...!U.)H..+.X..R.F.;E.w.k@G.pE[6...,d....P.z...s.YQ..@..6....~M.f`....,-.l=.....:.(...j7..7p...P|=...x..Kbl.....[..Y.s...FG.b.x...(.....Ol.)....,.p.....3jx..#X..2..*q...G...W(D~r..KuoH...@Toi[....*h"g.e...=.<g..W/.4.~.Z..tH....H.i.....;..om.C.5+S...E...../.V.,..&|...i....9W".~..&...,.?.w B.9.....}....7&.JjFU.....E'.....

C:\Users\user\AppData\Local\Temp\fonknpk

Process:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe

C:\Users\user\AppData\Local\Temp\fonknpk	
File Type:	data
Category:	dropped
Size (bytes):	60113
Entropy (8bit):	4.930356039937102
Encrypted:	false
SSDEEP:	1536:Fqa448V8tJKh6oKyLiTltDtnbBZdZzzzhxaWFg:0amCJKh6onaltDtn9nZzzWz
MD5:	E25AE6DAF4BB7B1AA0EF37BBC646B782
SHA1:	5C728BDBDC69527306370AECC6D5C268523F043B
SHA-256:	61CA2BDC62BD28E9B004B7F109F66FC8B0344A24FFDBF50EBBB0106A54865B01
SHA-512:	1A1DA41FDB905C7D54877E9E16F71FF37662BE2AB6A1C1E2AC46BC7600ECEB6323894839424C7A7A06C2FC366BB0A59F070BD56AD3CE1070335CBA56AB8805A
Malicious:	false
Reputation:	low
Preview:	U..!.....T...%.U...h.V...<.W...,.X...,.Y.....Z.....[...(.\.....]...n.^...0._...,.`.....a.....b...(.c.....d...(.e...x.f...#.g...,.h...,.i.....j.....k.....l...,.m...c.n.....o...d.p...<.q...,.r...,.s...,.t.....u.....v...H .w.....x.....y.....z.....{.....|...d.}...,.~.....2.....b.....,.....,.....,.....d.....d.....'.....P.....c.....l.....,.....,.....,..... .+.....+.....+.....p.....l.....,.....2.....p.....b.....,.....,.....p.....p.....l.....l.....'.....P.....c.....$.....,.....,.....,..... .....+.....+.....+.....x.....,.....2.....x.....b.....,.....,.....x

C:\Users\user\AppData\Local\Temp\nso6CF1.tmp	
Process:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
File Type:	data
Category:	dropped
Size (bytes):	709852
Entropy (8bit):	7.87001429899952
Encrypted:	false
SSDEEP:	12288:4Ph/JQuO9xgeB2Q54fr2dM4av0CGBmhFoqS3UDmhcOQV5eZTB6oI5BN:cdiuMxgy6frQuv0L0hFoqSkDmhcOsS98
MD5:	AEF5690996B3714098A9E0B69D9E5828
SHA1:	24B935683ECD3F3AF9F9EFE2620D6D05EFFED89C
SHA-256:	DBAADCC0481847BAB4237EDCF2F4990A047D5821BDFE186931103EAF17250101
SHA-512:	1F4A7C2FBD9553F7771B30CB907F7BAF3F4CF89450D9A79272250BA986CF92A249BE5E79827D332F709CEA8229EF37043F4236C626FDB82150EFD7AFE4D9DBE
Malicious:	false
Preview:	.S.....,.....T=.....S.....S..... .....J.....j.....q..... ....

C:\Users\user\AppData\Local\Temp\nso6CF2.tmp\System.dll	
Process:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\nso6CF2.tmp\System.dll	
Joe Sandbox View:	• Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse • Filename: PAYMENT CONFIRMATION.exe, Detection: malicious, Browse • Filename: PO187439.exe, Detection: malicious, Browse • Filename: 090009000000090.exe, Detection: malicious, Browse • Filename: NEWORDERLIST.exe, Detection: malicious, Browse • Filename: 00404000004.exe, Detection: malicious, Browse • Filename: 40900900090000.exe, Detection: malicious, Browse • Filename: INVO090090202.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.Injector.AIC.genEldorado.29599.exe, Detection: malicious, Browse • Filename: D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsx8F4E.tmp	
Process:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
File Type:	data
Category:	dropped
Size (bytes):	677854
Entropy (8bit):	7.91702747805609
Encrypted:	false
SSDEEP:	12288:4Ph/JQuO9xgeB2Q54fr2dM4av0CGBmhFoqS3UDmhcOQV5eZTB6oIL:cdiuMxgy6frQuv0L0hFoqSkDmhcOsS9a
MD5:	DD79AD8B5A51E756E3D0A2E149070DAA
SHA1:	9A999AE83C3078E311859D2AC02D97C8A95D4A51
SHA-256:	90B79E2B60E81A85EAFEA954724DD02BA7FAAF8CE63A3AD5C94BE5CDE5CE4256
SHA-512:	3F56D2AFEB344DC19DDEA59A8504366D1E118F2B4824CBC0E967D22BC2E616A726E7C846AABE7A3ED602B6328CB82A7338D4F97114DEC67FB896780A43E16DF
Malicious:	false
Preview:	.S.....,.....T=.....S.....S..... .....J.....j.....q..... ....

C:\Users\user\AppData\Local\Temp\nsz21EE.tmp	
Process:	C:\Users\user\Desktop\dYy3yfSkwY.exe
File Type:	data
Category:	dropped
Size (bytes):	709852
Entropy (8bit):	7.87001429899952
Encrypted:	false
SSDEEP:	12288:4Ph/JQuO9xgeB2Q54fr2dM4av0CGBmhFoqS3UDmhcOQV5eZTB6oI5BN:cdiuMxgy6frQuv0L0hFoqSkDmhcOsS98
MD5:	AEF5690996B3714098A9E0B69D9E5828
SHA1:	24B935683ECD3F3AF9F9EFE2620D6D05EFFED89C
SHA-256:	DBAADCC0481847BAB4237EDCF2F4990A047D5821BDFE186931103EAF17250101
SHA-512:	1F4A7C2FBD9553F7771B30CB907F7BAF3F4CF89450D9A79272250BA986CF92A249BE5E79827D332F709CEA8229EF37043F4236C626FDB82150EFD7AFE4D9DBE
Malicious:	false
Preview:	.S.....,.....T=.....S.....S..... .....J.....j.....q..... ....

C:\Users\user\AppData\Local\Temp\nsz21EF.tmp\System.dll	
Process:	C:\Users\user\Desktop\dYy3yfSkwY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsz21EF.tmp\System.dll	
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\dYy3yfSkwY.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:JR5tn:Rt
MD5:	537E946452ACB3A53CA8A63365818B7D
SHA1:	D0AB80082C59716C5C9A98284944590E5181BAE1
SHA-256:	F1C48C451E7B84D0CA328645EBBFCF632B9AA3ECAEE74FB36F3A84A2576B08FC
SHA-512:	2BF90A1A45B9F9A8351E3F1140C1D4151DABB3104F70C9C4A61F5CB43D0EECC1B2B6CD171A24899DDC1010ABA4BE450BFD46A101A3F7E05B86ED3935A5172763
Malicious:	**true**
Preview:	...|_,.H

C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe	
Process:	C:\Users\user\Desktop\dYy3yfSkwY.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	modified
Size (bytes):	682684
Entropy (8bit):	7.985587248644902
Encrypted:	false
SSDEEP:	12288:y4Bwh6Ga/zhQmHMbNdSsTIDy5dX5Z6fdBUd+YiUjBumJBP4/MW:y4B/Ga/zhQ0MhTUCdX5Z6fd24YZjkmJy
MD5:	3DEB8B7E51C21CBA0C2C723C5AF953DD
SHA1:	F98809B1B883912D278F7EAF64D7EEDFAEE1EF5A
SHA-256:	C0503F7C65391A5BE8030BBAAF6C17260FA67E40A3FCC23B84C26610C266008B
SHA-512:	27B12686A9979FD2107806B3C923F5E616FEA6F9DBFA0DBC1516FEE88C330B3DD81C82794E20F085FDF324E1EA4EFF9B4A942E55FB19F13CE1DBE24074E76A94
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L. .....K.....\.....<2.....p....@.....s.....p.....text... ZZ.....\..... ..`.rdata.....p.....`.....@..@.data.....r.....@....ndata.....@.....rsrc.....v.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.985587248644902

General

TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	dYy3yfSkwY.exe
File size:	682684
MD5:	3deb8b7e51c21cba0c2c723c5af953dd
SHA1:	f98809b1b883912d278f7eaf64d7eedfaee1ef5a
SHA256:	c0503f7c65391a5be8030bbaaf6c17260fa67e40a3fcc23b84c26610c266008b
SHA512:	27b12686a9979fd2107806b3c923f5e616fea6f9dbfa0dbc1516fee88c330b3dd81c82794e20f085fdf324e1ea4eff9b4a942e55fb19f13ce1dbe24074e76a94
SSDEEP:	12288:y4Bwh6Ga/zhQmHMbNdSsTIDy5dX5Z6fdBUd+YiUjBumJBP4/MW:y4B/Ga/zhQ0MhTUCdX5Z6fd24YZjkmJy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 15:31:32.181307077 CEST	192.168.2.7	8.8.8.8	0xcbed	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:38.392396927 CEST	192.168.2.7	8.8.8.8	0xc120	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:44.103826046 CEST	192.168.2.7	8.8.8.8	0x6d75	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:50.121778965 CEST	192.168.2.7	8.8.8.8	0xd449	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:50.405025959 CEST	192.168.2.7	8.8.4.4	0x13a9	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:51.727444887 CEST	192.168.2.7	8.8.8.8	0x6724	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:56.567003012 CEST	192.168.2.7	8.8.8.8	0x55d5	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:56.670478106 CEST	192.168.2.7	8.8.4.4	0x511	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:57.163907051 CEST	192.168.2.7	8.8.8.8	0x2c7f	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:01.350749016 CEST	192.168.2.7	8.8.8.8	0x8a28	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:01.448018074 CEST	192.168.2.7	8.8.4.4	0xe2cd	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:01.741183043 CEST	192.168.2.7	8.8.8.8	0x1878	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:06.151912928 CEST	192.168.2.7	8.8.8.8	0xb2e0	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:11.659318924 CEST	192.168.2.7	8.8.8.8	0x5e2e	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:17.732811928 CEST	192.168.2.7	8.8.8.8	0x96e4	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:23.874396086 CEST	192.168.2.7	8.8.8.8	0xd453	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:24.386266947 CEST	192.168.2.7	8.8.4.4	0xc18e	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 15:32:24.450488091 CEST	192.168.2.7	8.8.8.8	0x1ed3	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:29.021514893 CEST	192.168.2.7	8.8.8.8	0xe87c	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:29.627389908 CEST	192.168.2.7	8.8.4.4	0xb61b	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:30.022881985 CEST	192.168.2.7	8.8.8.8	0xfaff	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:34.235707998 CEST	192.168.2.7	8.8.8.8	0x9149	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:34.343688965 CEST	192.168.2.7	8.8.4.4	0x12e6	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:34.449165106 CEST	192.168.2.7	8.8.8.8	0xcd26	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:38.559259892 CEST	192.168.2.7	8.8.8.8	0x1154	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:44.031632900 CEST	192.168.2.7	8.8.8.8	0xd929	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:49.292860985 CEST	192.168.2.7	8.8.8.8	0x2e28	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:54.726989031 CEST	192.168.2.7	8.8.8.8	0x31d2	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:54.834827900 CEST	192.168.2.7	8.8.4.4	0x5b98	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:54.959928989 CEST	192.168.2.7	8.8.8.8	0x826d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:59.071983099 CEST	192.168.2.7	8.8.8.8	0x249c	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:59.138362885 CEST	192.168.2.7	8.8.4.4	0x19bb	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:59.245536089 CEST	192.168.2.7	8.8.8.8	0x9170	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:03.369879961 CEST	192.168.2.7	8.8.8.8	0x20ef	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:03.432816029 CEST	192.168.2.7	8.8.4.4	0xe0ac	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:03.528409958 CEST	192.168.2.7	8.8.8.8	0xbe2b	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:07.648883104 CEST	192.168.2.7	8.8.8.8	0xd36	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:12.904831886 CEST	192.168.2.7	8.8.8.8	0x308e	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:18.322038889 CEST	192.168.2.7	8.8.8.8	0x6a52	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:23.732136011 CEST	192.168.2.7	8.8.8.8	0x9e46	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:23.784437895 CEST	192.168.2.7	8.8.4.4	0xd2da	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:24.804606915 CEST	192.168.2.7	8.8.4.4	0xd2da	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:24.870029926 CEST	192.168.2.7	8.8.8.8	0x93b6	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:28.934925079 CEST	192.168.2.7	8.8.8.8	0x88c6	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:28.995167971 CEST	192.168.2.7	8.8.4.4	0x32f7	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:29.060477018 CEST	192.168.2.7	8.8.8.8	0x63cf	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:33.122565985 CEST	192.168.2.7	8.8.8.8	0x3f68	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:33.182643890 CEST	192.168.2.7	8.8.4.4	0xcf42	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:33.247688055 CEST	192.168.2.7	8.8.8.8	0xc9fb	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:37.327805996 CEST	192.168.2.7	8.8.8.8	0x8b83	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:42.529644012 CEST	192.168.2.7	8.8.8.8	0xb5ed	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:47.733093977 CEST	192.168.2.7	8.8.8.8	0x4f3f	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:52.950977087 CEST	192.168.2.7	8.8.8.8	0x8b88	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:53.011431932 CEST	192.168.2.7	8.8.4.4	0x2aae	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 15:33:53.083364010 CEST	192.168.2.7	8.8.8.8	0x6cee	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:57.159787893 CEST	192.168.2.7	8.8.8.8	0x2987	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:57.220031977 CEST	192.168.2.7	8.8.4.4	0x97ed	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:57.286722898 CEST	192.168.2.7	8.8.8.8	0xab9d	Standard query (0)	wekeepworking12.sytes.net	A (IP address)	IN (0x0001)

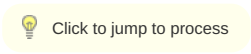
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 15:31:32.241700888 CEST	8.8.8.8	192.168.2.7	0xcbed	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:38.456140041 CEST	8.8.8.8	192.168.2.7	0xc120	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:31:44.165118933 CEST	8.8.8.8	192.168.2.7	0x6d75	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:06.210746050 CEST	8.8.8.8	192.168.2.7	0xb2e0	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:11.717715979 CEST	8.8.8.8	192.168.2.7	0x5e2e	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:17.791794062 CEST	8.8.8.8	192.168.2.7	0x96e4	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:38.619369984 CEST	8.8.8.8	192.168.2.7	0x1154	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:44.094465971 CEST	8.8.8.8	192.168.2.7	0xd929	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:32:49.351901054 CEST	8.8.8.8	192.168.2.7	0x2e28	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:07.710572958 CEST	8.8.8.8	192.168.2.7	0xd36	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:12.966074944 CEST	8.8.8.8	192.168.2.7	0x308e	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:18.380691051 CEST	8.8.8.8	192.168.2.7	0x6a52	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:37.386540890 CEST	8.8.8.8	192.168.2.7	0x8b83	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:42.590915918 CEST	8.8.8.8	192.168.2.7	0xb5ed	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 10, 2021 15:33:47.793531895 CEST	8.8.8.8	192.168.2.7	0x4f3f	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: dYy3yfSkwY.exe PID: 6108 Parent PID: 5724

General

Start time:	15:31:16
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\dYy3yfSkwY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dYy3yfSkwY.exe'
Imagebase:	0x400000
File size:	682684 bytes
MD5 hash:	3DEB8B7E51C21CBA0C2C723C5AF953DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.254544184.0000000002180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254544184.0000000002180000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254544184.0000000002180000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: dYy3yfSkwY.exe PID: 668 Parent PID: 6108

General

Start time:	15:31:22
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\dYy3yfSkwY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dYy3yfSkwY.exe'
Imagebase:	0x400000
File size:	682684 bytes
MD5 hash:	3DEB8B7E51C21CBA0C2C723C5AF953DD
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: 00000003.00000001.251399209.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000001.251399209.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000001.251399209.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: opjlpsercy.exe PID: 3724 Parent PID: 3292

General

Start time:	15:31:35
Start date:	10/06/2021
Path:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe'
Imagebase:	0x400000
File size:	682684 bytes
MD5 hash:	3DEB8B7E51C21CBA0C2C723C5AF953DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.308184070.0000000009810000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.308184070.0000000009810000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.308184070.0000000009810000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: opjlpsercy.exe PID: 4520 Parent PID: 3724

General

Start time:	15:31:42
Start date:	10/06/2021
Path:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe'
Imagebase:	0x400000
File size:	682684 bytes
MD5 hash:	3DEB8B7E51C21CBA0C2C723C5AF953DD
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: 0000000B.00000002.317958007.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.317958007.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.317958007.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.319773965.000000000396D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.319773965.000000000396D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.319549745.00000000028EE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.320311850.0000000004B02000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.320311850.0000000004B02000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.320311850.0000000004B02000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000001.299993586.0000000000414000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000001.299993586.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000001.299993586.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.320200858.0000000004A70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.320200858.0000000004A70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.320200858.0000000004A70000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.320200858.0000000004A70000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.320124108.00000000049E7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.320124108.00000000049E7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.320124108.00000000049E7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.319677498.00000000038E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.319677498.00000000038E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.319677498.00000000038E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: opjlpsercy.exe PID: 5892 Parent PID: 3292

General

Start time:	15:31:43
Start date:	10/06/2021
Path:	C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\monsuyajo\opjlpsercy.exe'
Imagebase:	0x400000
File size:	682684 bytes
MD5 hash:	3DEB8B7E51C21CBA0C2C723C5AF953DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis