ID: 560236
Sample Name: ZgzIenrtf5.exe
Cookbook: default.jbs
Time: 09:45:02
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ZgzIenrtf5.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
AV Detection 7
E-Banking Fraud 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Jbx Signature Overview 7
AV Detection 7
Networking 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 11
General Information 12
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat 13
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 13
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak 13
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin 14
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat 14
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 17
Sections 17
Resources 17
Imports 17
Network Behavior 18
Snort IDS Alerts 18
TCP Packets 18
Statistics 20

System Behavior 20
Analysis Process: ZgzIenrtf5.exePID: 3764, Parent PID: 1340 20
General 20
File Activities 21
File Created 21
File Deleted 21
File Written 22
File Read 23
Disassembly 23

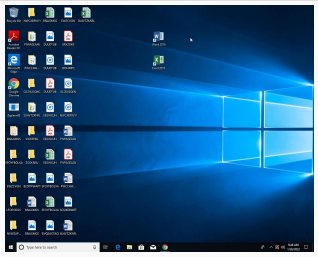
Windows Analysis Report

Zgzlenrtf5.exe

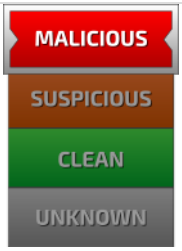
Overview

General Information

Sample Name:	Zgzlenrtf5.exe
Analysis ID:	560236
MD5:	03efbc1aa78259..
SHA1:	3877473e9e9014.
SHA256:	c5d68d3abd9d6f..
Tags:	exe NanoCore RAT
Infos:	



Detection



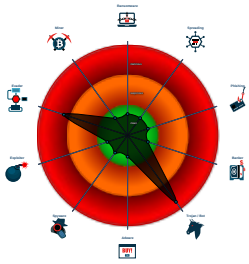
Nanocore

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- Zgzlenrtf5.exe (PID: 3764 cmdline: "C:\Users\user\Desktop\Zgzlenrtf5.exe" MD5: 03EFBC1AA782599E235F4C1B0303FFB1)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "4189f41b-a3e5-405b-b524-4758becc",
  "Group": "2022",
  "Domain1": "107.173.60.45",
  "Domain2": "sys2021.linkpc.net",
  "Port": 54955,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ZgzIenrtf5.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
ZgzIenrtf5.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
ZgzIenrtf5.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
ZgzIenrtf5.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.253185094.0000000000AE2000.00000002.00000001.01000000.00000003.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000000.00000000.253185094.0000000000AE2000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.253185094.0000000000AE2000.00000002.00000001.01000000.00000003.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000003.266607534.00000000045D4000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x170a:$a: NanoCore • 0x172f:$a: NanoCore • 0x1788:$a: NanoCore • 0x11925:$a: NanoCore • 0x1194b:$a: NanoCore • 0x119a7:$a: NanoCore • 0x1e7fc:$a: NanoCore • 0x1e855:$a: NanoCore • 0x1e888:$a: NanoCore • 0x1eab4:$a: NanoCore • 0x1eb30:$a: NanoCore • 0x1f149:$a: NanoCore • 0x1f292:$a: NanoCore • 0x1f766:$a: NanoCore • 0x1fa4d:$a: NanoCore • 0x1fa64:$a: NanoCore • 0x22ded:$a: NanoCore • 0x241a7:$a: NanoCore • 0x241f1:$a: NanoCore • 0x24e4b:$a: NanoCore • 0x2a430:$a: NanoCore
Process Memory Space: ZgzIenrtf5.exe PID: 3764	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x99a3d:$x1: NanoCore.ClientPluginHost • 0x111ad1:$x1: NanoCore.ClientPluginHost • 0x99a67:$x2: IClientNetworkHost • 0x111b0e:$x2: IClientNetworkHost • 0x1155ff:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x120685:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.ZgzIenrtf5.exe.45dcda6.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
0.3.ZgzIenrtf5.exe.45dcda6.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
0.3.ZgzIenrtf5.exe.45f6dff.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3831:$x1: NanoCore.ClientPluginHost • 0x386a:$x2: IClientNetworkHost
0.3.ZgzIenrtf5.exe.45f6dff.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3831:$x2: NanoCore.ClientPluginHost • 0x394c:$s4: PipeCreated • 0x384b:$s5: IClientLoggingHost
0.0.ZgzIenrtf5.exe.ae0000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 6 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

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

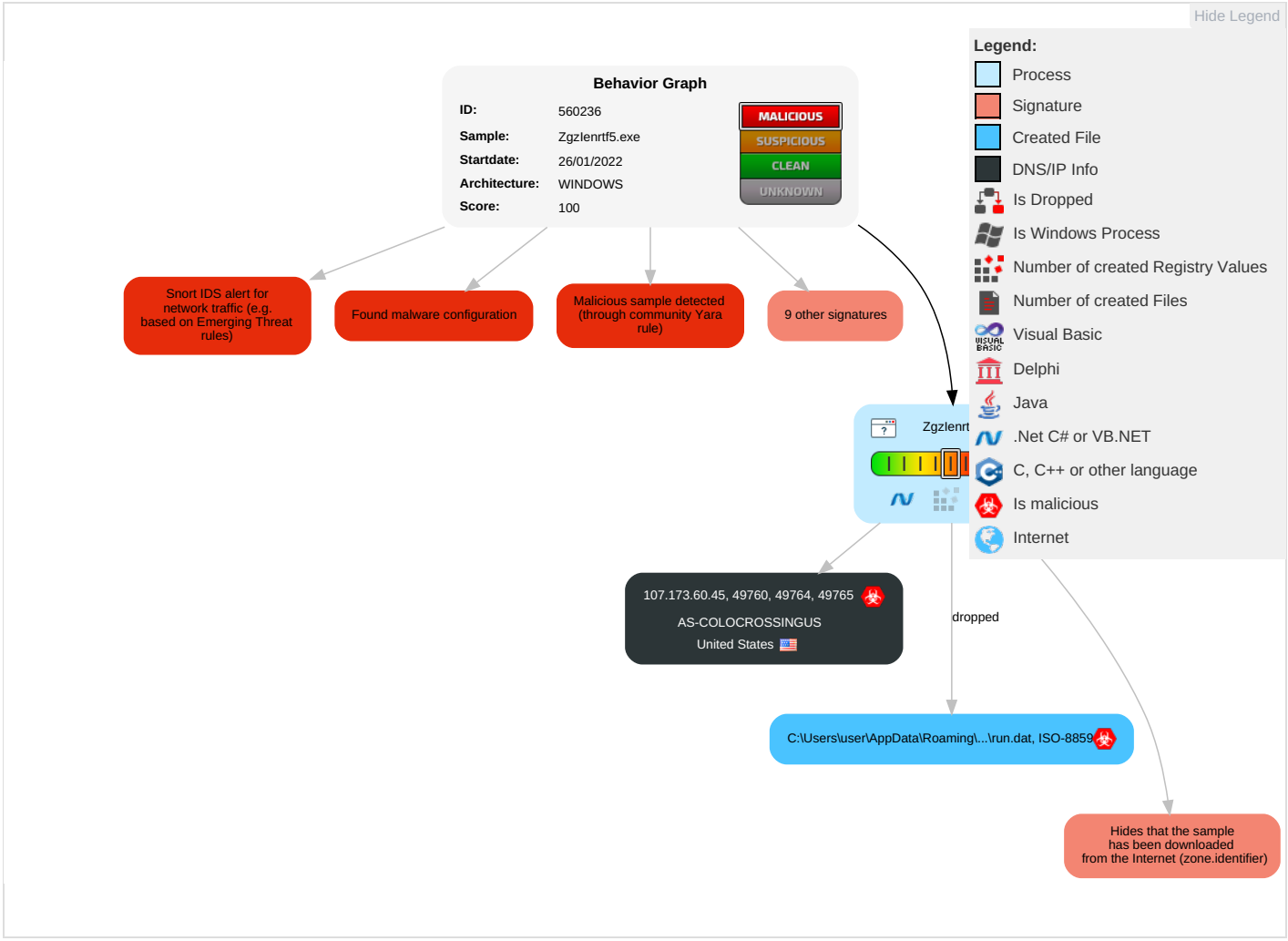
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
Zgzlenrtf5.exe	87%	Virustotal		Browse
Zgzlenrtf5.exe	85%	Metadefender		Browse
Zgzlenrtf5.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
Zgzlenrtf5.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
Zgzlenrtf5.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Zgzlenrtf5.exe.ae0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
107.173.60.45	1%	Virustotal		Browse
107.173.60.45	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

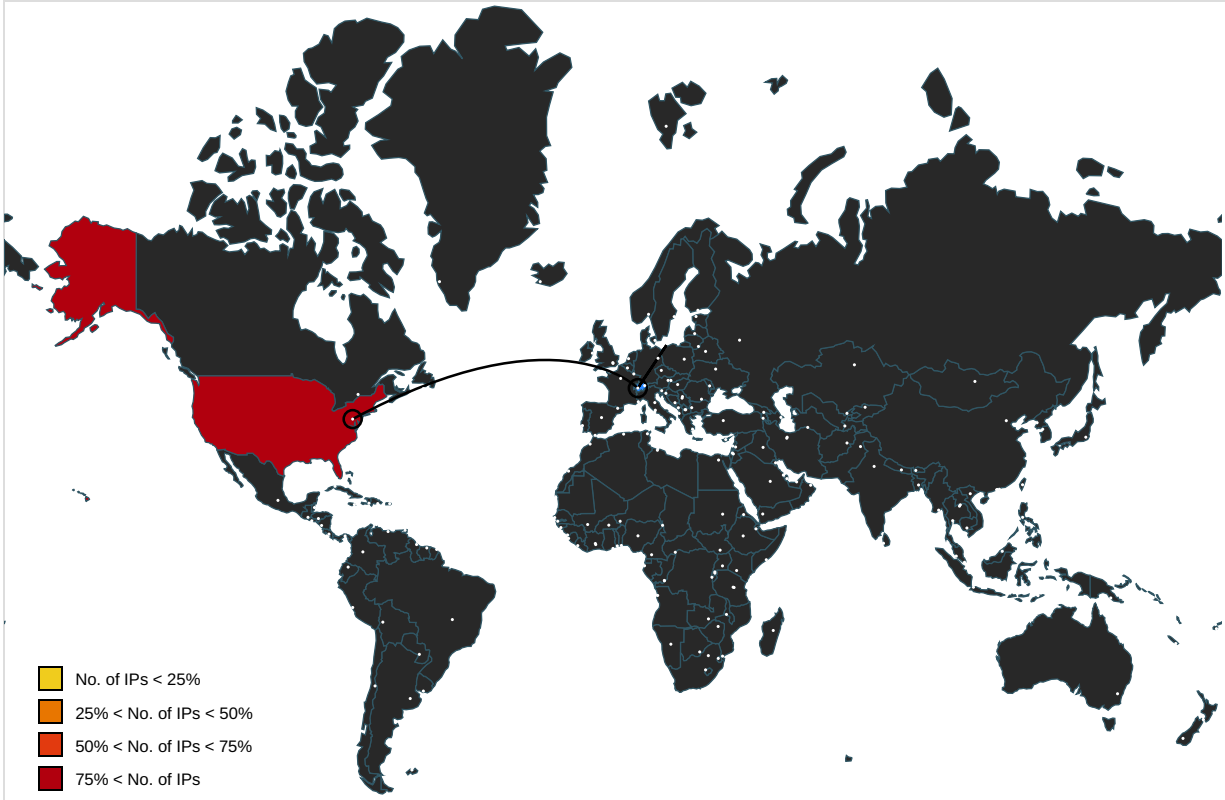
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
107.173.60.45	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
sys2021.linkpc.net	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	ZgzIenrtf5.exe, 00000000.00000003.266607534.00000000045D4000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.173.60.45	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560236
Start date:	26.01.2022
Start time:	09:45:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZgzIenrtf5.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:	22
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@1/5@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
09:46:06	API Interceptor	972x Sleep call for process: ZgzIenrtf5.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\ZgzIenrtf5.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\ZgzIenrtf5.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:dfl:d9
MD5:	74D04D3CBC86F9FA0D26B5D5CA6F3765
SHA1:	EF3A51C5729BF22CFB8B1AECDC51063879D1170A
SHA-256:	7F87D5B04B82515C9271FC7746408DBB028581F2F0EDA62599FDE036B80E8516
SHA-512:	3F8E9260A3942BD6E0FEC80DFDD92471AB1A0A7B6DF6D7D502DD8A059F132AE804EF04AAC473862EC7E14DF1725EA777D0276A7975B8AD1D94324352B6F7220
Malicious:	**true**
Reputation:	low
Preview:	{.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak

Process:	C:\Users\user\Desktop\ZgzIenrtf5.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823

Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\Desktop\ZgzIenrtf5.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat

Process:	C:\Users\user\Desktop\ZgzIenrtf5.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9..j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.44950897695562
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	ZgzIenrtf5.exe

File size:	207360
MD5:	03efbc1aa782599e235f4c1b0303ffb1
SHA1:	3877473e9e9014bc8eee7782dc81345772e832f9
SHA256:	c5d68d3abd9d6f9b094ea1bdb064ca709cc54de13f86856c4ffe34c64148c87c
SHA512:	15ac77a5d18d1820a1fa72bcb74b13fe1eeffc12d0899af4a8da94d3abe3947dfbf2a55258d896ee76cb9dd50717e2738daea2a630bbe80e00c0d1ad90319511
SSDEEP:	6144:gLV6Bta6dtJmakIM5D6xUtdHfBTQxVqtjreE:gLV6Btpmkxkd/FcVqx9
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....'.T.....................`........... ....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x15da0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	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	0x1c798	0x1c800	False	0.594512404057	data	6.59808579998	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15da0	0x15e00	False	0.999866071429	data	7.99790613337	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x15d48	TIM image, Pixel at (56860,48781) Size=63345x11644		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-09:46:08.216157	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:14.116786	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:18.682717	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:23.198746	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:27.683212	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:34.008137	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:38.414028	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:42.949617	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:49.268783	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	54955	192.168.2.7	107.173.60.45
01/26/22-09:46:55.337640	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:01.657634	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:07.950589	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:13.975269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:20.932232	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:27.448467	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:35.133123	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:41.265641	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49835	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:47.299230	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:53.344216	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49851	54955	192.168.2.7	107.173.60.45
01/26/22-09:47:59.343769	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	54955	192.168.2.7	107.173.60.45
01/26/22-09:48:03.797518	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49865	54955	192.168.2.7	107.173.60.45
01/26/22-09:48:09.718980	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49866	54955	192.168.2.7	107.173.60.45

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:46:07.985819101 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:08.101031065 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:08.101176977 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:08.216156960 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:08.361574888 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:08.361695051 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:08.531954050 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:08.532068968 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:08.647684097 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:08.647931099 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:08.828762054 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:08.828849077 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.000732899 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.000848055 CET	49760	54955	192.168.2.7	107.173.60.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:46:09.169156075 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.169193983 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.169219017 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.169240952 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.169286013 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.169306993 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.284141064 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284171104 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284183979 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284197092 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284218073 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284231901 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284246922 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284264088 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.284272909 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.284296036 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.284439087 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.399014950 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399044037 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399060965 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399077892 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399094105 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399108887 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399126053 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399142027 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399162054 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399184942 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399199963 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399215937 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399229050 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399234056 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.399245024 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399252892 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.399262905 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399272919 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.399280071 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.399327993 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.399333000 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514070034 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514096975 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514115095 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514137983 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514153957 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514158010 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514177084 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514182091 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514197111 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514214993 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514231920 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514249086 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514249086 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514266014 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514282942 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514295101 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514298916 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514298916 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514317036 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514333963 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514352083 CET	54955	49760	107.173.60.45	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:46:09.514369011 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514379978 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514384985 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514384985 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514401913 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514417887 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514430046 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514432907 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514434099 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514451981 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514467955 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514483929 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514501095 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514516115 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514518976 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514523983 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514533997 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514550924 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514566898 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.514570951 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514575005 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514626026 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.514628887 CET	49760	54955	192.168.2.7	107.173.60.45
Jan 26, 2022 09:46:09.629300117 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.629331112 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.629350901 CET	54955	49760	107.173.60.45	192.168.2.7
Jan 26, 2022 09:46:09.629373074 CET	54955	49760	107.173.60.45	192.168.2.7

Statistics

No statistics

System Behavior

Analysis Process: ZgzIenrtf5.exe PID: **3764**, Parent PID: **1340**

General

Target ID:	0
Start time:	09:46:03
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\ZgzIenrtf5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ZgzIenrtf5.exe"
Imagebase:	0xae0000
File size:	207360 bytes
MD5 hash:	03EFBC1AA782599E235F4C1B0303FFB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.253185094.0000000000AE2000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.253185094.0000000000AE2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.253185094.0000000000AE2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.266607534.00000000045D4000.00000004.00000800.00020000.00000000.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\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	54007A1	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	540089B	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	54007A1	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	54007A1	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	1	540089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	540089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	540089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	540355C	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ZgzIenrtf5.exe:Zone.Identifier	success or wait	1	5400B41	DeleteFileA
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	130BF0E	DeleteFileW

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	0	8	7b 2b fd fd fd fd 48	{H	success or wait	1	5400A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	1	5400A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	426832	fd fd 67 26 6a 6f 1f 01 fd 49 50 67 08 fd 62 47 4d 64 fd 0d fd 52 3e 69 fd fd 09 6f fd fd 04 49 fd 3e f0 26 fd 72 7b fd fd fd fd 38 fd e5 fd 7d fd 89 fd 45 03 7f fd fd 76 fd 21 37 fd 75 33 65 fd fd 20 fd fd 05 fd fd 64 62 fd fd 15 7d fd fd 1d 02 02 fd fd 22 fd 74 28 06 78 43 39 fd 63 70 15 42 fd fd fd fd 37 fd 0f 1b 27 fd fd fd fd fd 7f fd 25 fd 09 fd 06 fd fd 77 fd 5e fd fd 5f 13 fd fd 02 1d 34 fd 42 fd 57 25 fd 3c a6 64 69 fd 30 fd 7b 39 fd 78 53 fd fd fd 35 fd fd fd 29 05 fd 77 fd 0f 24 14 fd 43 fd fd 3f 60 46 cf fd 75 fd 35 d2 54 fd 58 fd 77 27 53 69 fd fd 7a fd 6e 7b fd fd c4 59 21 6d fd fd 1c 52 41 fd fd fd 78 67 fd 3a 03 fd 5b 37 fd 18 fd 7a fd fd 39 40 02 4b fd 2d fd fd fd 54 fd fd 2b fd 41 43 65	g&joIPgGMR>ioI>&r{8}E v!7u3e db }"t(xC9cpB7'%w^_BW% <i0{9xS5)w$C? `Fu5TXw'Sizn{Y!mRAxg[7z9@K-T+ACe	success or wait	1	5400A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	3	5400A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd	9iH}Z4f~a	success or wait	2	5400A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 4a 22 fd 43 3b 22 61	9iH}Z4fJ"C;"a	success or wait	1	540355C	CopyFileW

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
C:\Users\user\Desktop\ZgzIenrtf5.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Users\user\Desktop\ZgzIenrtf5.exe	unknown	512	success or wait	1	7253BF06	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	5400A53	ReadFile

Disassembly

No disassembly