ID: 433263
Sample Name: ORDER.exe
Cookbook: default.jbs
Time: 14:58:20
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

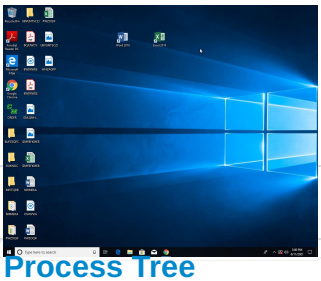
Analysis Report ORDER.exe

Overview

General Information

Sample Name:	ORDER.exe
Analysis ID:	433263
MD5:	425f6b1e9437b1f..
SHA1:	65cf68fdda68b03..
SHA256:	cfb1e4b65fc8e0d..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

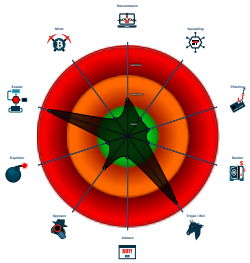
Nanocore

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 dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- ORDER.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\ORDER.exe' MD5: 425F6B1E9437B1F1DB352D1393D236D5)
  - schtasks.exe (PID: 6920 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\Odstcl' /XML 'C:\Users\user\AppData\Local\Temp\tmp6A1C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ORDER.exe (PID: 7148 cmdline: {path} MD5: 425F6B1E9437B1F1DB352D1393D236D5)
    - schtasks.exe (PID: 4388 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp777A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ORDER.exe (PID: 6044 cmdline: C:\Users\user\Desktop\ORDER.exe 0 MD5: 425F6B1E9437B1F1DB352D1393D236D5)
  - schtasks.exe (PID: 7116 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\Odstcl' /XML 'C:\Users\user\AppData\Local\Temp\tmpFE00.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ORDER.exe (PID: 4480 cmdline: {path} MD5: 425F6B1E9437B1F1DB352D1393D236D5)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "30b6fbac-dd0d-47bd-b8ab-6df66b01",
  "Group": "Default",
  "Domain1": "kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu",
  "Domain2": "",
  "Port": 1187,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.906988359.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000D.00000002.906988359.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000002.906988359.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000010.00000002.815063432.0000000003D01000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x116d1d:$x1: NanoCore.ClientPluginHost • 0x14973d:$x1: NanoCore.ClientPluginHost • 0x116d5a:$x2: IClientNetworkHost • 0x14977a:$x2: IClientNetworkHost • 0x11a88d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x14d2ad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000010.00000002.815063432.0000000003D0 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 44 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.ORDER.exe.2b93884.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
24.2.ORDER.exe.2b93884.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
16.2.ORDER.exe.3e07b90.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
16.2.ORDER.exe.3e07b90.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
16.2.ORDER.exe.3e07b90.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 82 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

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

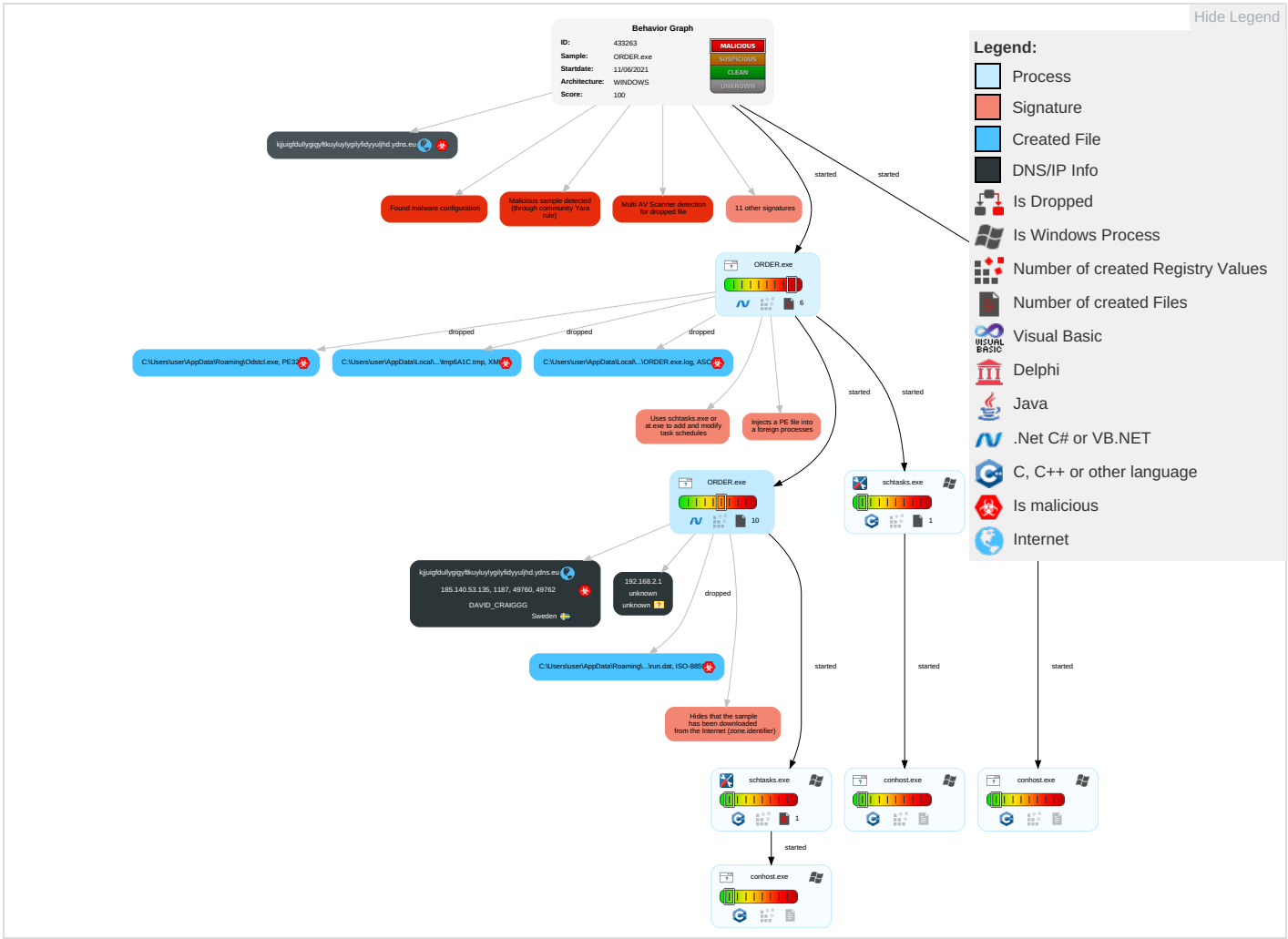
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

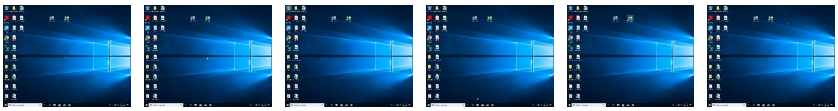
Behavior Graph



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
ORDER.exe	33%	Virustotal		Browse
ORDER.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Odstcl.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.ORDER.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
24.0.ORDER.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.ORDER.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
24.0.ORDER.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.ORDER.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.ORDER.exe.59c0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.2.ORDER.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://en.wl	0%	Avira URL Cloud	safe	
http://www.fonts.comro	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr2Dq	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comMd	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.founder.com.cn/cngH	0%	Avira URL Cloud	safe	
http://en.wa	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/c	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.com9	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.com(G	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnt-p	0%	Avira URL Cloud	safe	
http://www.carterandcone.comtal	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comTC3	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.comF(G	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comnewk	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalicLG$	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexc	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.sandoll.co.kr;D~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlic	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com-d	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-c	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.tiro.comFTd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comhly	0%	Avira URL Cloud	safe	
http://www.carterandcone.comy	0%	URL Reputation	safe	
http://www.carterandcone.comy	0%	URL Reputation	safe	
http://www.carterandcone.comy	0%	URL Reputation	safe	
http://www.fontbureau.comuec:G~	0%	Avira URL Cloud	safe	
kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.comona	0%	Avira URL Cloud	safe	
http://www.tiro.comn7dc	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu	185.140.53.135	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.135	kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433263
Start date:	11.06.2021
Start time:	14:58:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/7@16/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:59:49	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\ORDER.exe" s>$(Arg0)
14:59:49	API Interceptor	689x Sleep call for process: ORDER.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.135	CONTRACT.exe	Get hash	malicious	Browse	
	Swift.exe	Get hash	malicious	Browse	
	5U8Z6pqTlhp68RB.exe	Get hash	malicious	Browse	
	HY_RAY_RFQ,pdf .exe	Get hash	malicious	Browse	
	Shipping_Documents_INV_PL_and_BL,pdf.exe	Get hash	malicious	Browse	
	Geno_Quotation,pdf.exe	Get hash	malicious	Browse	
	PO20002106.exe	Get hash	malicious	Browse	
	SOA_30_11_2020,pdf.exe	Get hash	malicious	Browse	
	20201229_QUA_20Y0252,pdf.exe	Get hash	malicious	Browse	
	PO029734,pdf.exe	Get hash	malicious	Browse	
	VSI_202012223,pdf.exe	Get hash	malicious	Browse	
	PO968_8359808,pdf.exe	Get hash	malicious	Browse	
	purchase order # 10000000648.pdf.exe	Get hash	malicious	Browse	
	Order 20015639 15-10-2020,pdf.exe	Get hash	malicious	Browse	
	shipping documents.doc	Get hash	malicious	Browse	
	POEA-MANNING ADVISORY 2020-56.PDF.exe	Get hash	malicious	Browse	
	Doc_1110_090820.exe	Get hash	malicious	Browse	
	Doc0_01210_72820.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
kjjuigfdullygigyftkuyluylygilyfidyyuljhd.ydns.eu	CONTRACT.exe	Get hash	malicious	Browse	• 185.140.53.135
	Swift.exe	Get hash	malicious	Browse	• 185.140.53.135
	5U8Z6pqTlhp68RB.exe	Get hash	malicious	Browse	• 185.140.53.135

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	ORDER-21611docx.exe	Get hash	malicious	Browse	• 185.165.153.116
	6VYNUalwUt.exe	Get hash	malicious	Browse	• 185.244.30.92
	ORDER-6010.pdf.exe	Get hash	malicious	Browse	• 185.244.30.92
	CONTRACT.exe	Get hash	malicious	Browse	• 185.140.53.135
	doc030273202105211733O5IMG0012.exe	Get hash	malicious	Browse	• 185.140.53.230
	yfilQwrYpA.exe	Get hash	malicious	Browse	• 185.140.53.216
	Ff6m4N8pog.exe	Get hash	malicious	Browse	• 185.140.53.216
	yCdBrRiAN2.exe	Get hash	malicious	Browse	• 185.140.53.216
	loKHQzx6Lf.exe	Get hash	malicious	Browse	• 185.140.53.216
	SecuriteInfo.com.Program.Win32.Wacapew.Cml.7225.exe	Get hash	malicious	Browse	• 185.140.53.129
	Shipping Documents_Bill of Lading 910571880.exe	Get hash	malicious	Browse	• 185.140.53.129
	knqh5Hw6gu.exe	Get hash	malicious	Browse	• 185.140.53.13
	Container_Deposit_slip_pdf.jar	Get hash	malicious	Browse	• 185.244.30.47
	Cargo Charter Request details.vbs	Get hash	malicious	Browse	• 185.244.30.184
	Shipping Documents_Bill of Lading 910571880,pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	WarkZh7G8j6Xo8r.exe	Get hash	malicious	Browse	• 91.193.75.66
	Re R new proforma.exe	Get hash	malicious	Browse	• 185.140.53.138

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO20880538.exe	Get hash	malicious	Browse	• 185.140.53.129
	QI5MR3pte0.exe	Get hash	malicious	Browse	• 185.140.53.40
	5Em2NXNxSt.exe	Get hash	malicious	Browse	• 185.140.53.40

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Temp\tmp6A1C.tmp

Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.168844125271163
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGHBtn:cbhK79lNQR/rydbz9I3YODOLNdq38
MD5:	F8CF011BF6E5580EAE43A61562FFE6F0
SHA1:	595C40DE064CF3E87D5266529C2E0F5A0277F020
SHA-256:	7EE91880594E206246BE39C4348D060546A40D200AF3213CC7DFBCB9848F84AA
SHA-512:	72ABBE277F95CB790031FF7639B3123202E312908839ABCE6A2EB957D164D5964C1DE924C7A9DC47F11D03EDBE61E93D7DCD2057CDB02113B783D0240F1BE9
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp777A.tmp

Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1295
Entropy (8bit):	5.09846064283307
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YVlxtn:cbk4oL600QydbQxIYODOLedq3Hj
MD5:	8F1E8C51D91DF67169BEE20FF3FFEAF6

C:\Users\user\AppData\Local\Temp\tmp777A.tmp

SHA1:	032E2A290F6D69952BB614F1C2CC33B755854FF5
SHA-256:	DF437CB636EA881017FD876748F164EEA207D89695EB6F6E5A3C9BD1F0215E1C
SHA-512:	8311E6829EC9343284E7E414FD4B555EDD37681F35ED4440A306093A0D69EE90E7811A8235966A7F8AB055D6718B99A0A99D34BA6F75C7CD0FFEBC988D1D60B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpFE00.tmp

Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.168844125271163
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGHBtn:cbhK79lNQR/rydbz9I3YODOLNdq38
MD5:	F8CF011BF6E5580EAE43A61562FFE6F0
SHA1:	595C40DE064CF3E87D5266529C2E0F5A0277F020
SHA-256:	7EE91880594E206246BE39C4348D060546A40D200AF3213CC7DFBCB9848F84AA
SHA-512:	72ABBE277F95CB790031FF7639B3123202E312908839ABCE6A2EB957D164D5964C1DE924C7A9DC47F11D03EDBE61E93D7DCD2057CDB02113B783D0240F1BE9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

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

Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:t9+:P+
MD5:	9E9C776D1074DFE1E684AAD1D917A727
SHA1:	D995B8935AAFCA0E412C630EF4FF101C653A3785
SHA-256:	EE168FBC34E8D827CED4BFCD72848540E46F7F9475BA50D46E7A724BD47E2911
SHA-512:	7469C097FEDFA9160EC245F31627CB45F6402E3F4C2DDD5CC9C8BA81FCCB6BEEAA7787A493783A59CECE8881A960E47004058349CDDDA90CF3D7263B7DC441E
Malicious:	**true**
Reputation:	low
Preview:	-N`..,.H

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

Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	32
Entropy (8bit):	3.9496987351738495
Encrypted:	false
SSDEEP:	3:oNt+WfWqG3Jn:oNwvqgJ
MD5:	F2F2E9E658CF35F1C5999C1870420D3C
SHA1:	42D5DE29AA59D9860FAFD167334DC3BED9586484
SHA-256:	AEB7B972FF18BCA62298F2BD912F8E8AC68337A714F1E868208AECC480301F99
SHA-512:	078F5697674727E038177A5A09D2FEDD0AC5474B157C346155F29A8119F49CC49B3C09C861E50404CD3D03031734968A0C796785E0696C5E694433304F15ACA0
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Preview:	C:\Users\user\Desktop\ORDER.exe

C:\Users\user\AppData\Roaming\Odstcl.exe	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	536064
Entropy (8bit):	7.699438756547545
Encrypted:	false
SSDEEP:	12288:SwbjmMziWZrnoSSmaLBWIRqzPc/yt7ZX9HqUSagcq:q6jd9IcUyt7ZX5DSjc
MD5:	425F6B1E9437B1F1DB352D1393D236D5
SHA1:	65CF68FDDA68B0327D51B7E3989AFAA2258D4C6D
SHA-256:	CFB1E4B65FC8E0D9CA698AB5E67FC77735880B8439A6F4EE4E48BE06CA631DC2
SHA-512:	EACCC681B25DDD203B0A79ECBFA1E464B129066F7090069BDB7D5F9D4955A57D86F1D76441F2E141BFEA1E249B8A43C8AED527EC18B5238066F75CFDFB7948 5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 46%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....~7... ...@....@.. ..... ..@.....,7..O....@..\.....`..... ....H.....text..... ....`.rsrc...\....@.....@..@.rel oc.....`.....,.....@..B.....`7.....H.....@...L.....?....v.....^.(.....}.....}....*.0.....t.....t.....o.....{....o....o.....o.....{....o....o.....o.....{... .o....o.....o.....{....o....o.....(.....{.....,....e..+.....+...*..0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{....r...po.....{.....(....o.....{.....(....o.....{.....(....o.....*..0..._.....(..... (.....o.....,)....t.....o....r!..p(.....,..o....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.699438756547545
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ORDER.exe
File size:	536064
MD5:	425f6b1e9437b1f1db352d1393d236d5
SHA1:	65cf68fdda68b0327d51b7e3989afaa2258d4c6d
SHA256:	cfb1e4b65fc8e0d9ca698ab5e67fc77735880b8439a6f4ee4e48be06ca631dc2
SHA512:	eaccc681b25ddd203b0a79ecbfa1e464b129066f7090069bdb7d5f9d4955a57d86f1d76441f2e141bfea1e249b8a43c8aed527ec18b5238066f75cfdfb794805
SSDEEP:	12288:SwbjmMziWZrnoSSmaLBWIRqzPc/yt7ZX9HqUSagcq:q6jd9IcUyt7ZX5DSjc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....~7... ...@....@.. ....@.....

File Icon

Icon Hash:	18da1abcb2d2d2b0

Static PE Info

General	
Entrypoint:	0x48377e
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C2CD9C [Fri Jun 11 02:42:36 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x81784	0x81800	False	0.877169929416	data	7.72970366103	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x105c	0x1200	False	0.270182291667	data	2.85061195999	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 14:59:51.571542978 CEST	192.168.2.4	8.8.8.8	0x3080	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 14:59:57.756336927 CEST	192.168.2.4	8.8.8.8	0xba23	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:03.267348051 CEST	192.168.2.4	8.8.8.8	0x28d6	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:00:08.865986109 CEST	192.168.2.4	8.8.8.8	0x3673	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:14.500823021 CEST	192.168.2.4	8.8.8.8	0x1d3	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:20.230350971 CEST	192.168.2.4	8.8.8.8	0xe2dd	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:25.817883968 CEST	192.168.2.4	8.8.8.8	0xf2b8	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:31.360760927 CEST	192.168.2.4	8.8.8.8	0xfb1f	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:36.962040901 CEST	192.168.2.4	8.8.8.8	0xd864	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:42.678448915 CEST	192.168.2.4	8.8.8.8	0xb4f7	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:48.290079117 CEST	192.168.2.4	8.8.8.8	0x8a93	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:53.909318924 CEST	192.168.2.4	8.8.8.8	0xbb18	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:59.440179110 CEST	192.168.2.4	8.8.8.8	0x6dbc	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:01:05.206954002 CEST	192.168.2.4	8.8.8.8	0xd178	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:01:10.730623960 CEST	192.168.2.4	8.8.8.8	0x74e6	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:01:15.981034994 CEST	192.168.2.4	8.8.8.8	0xbc5c	Standard query (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd.ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

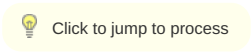
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 14:59:51.638654947 CEST	8.8.8.8	192.168.2.4	0x3080	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 14:59:57.837124109 CEST	8.8.8.8	192.168.2.4	0xba23	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:03.325910091 CEST	8.8.8.8	192.168.2.4	0x28d6	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:08.924860954 CEST	8.8.8.8	192.168.2.4	0x3673	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:14.562788010 CEST	8.8.8.8	192.168.2.4	0x1d3	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:00:20.290426970 CEST	8.8.8.8	192.168.2.4	0xe2dd	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:25.877048016 CEST	8.8.8.8	192.168.2.4	0xf2b8	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:31.420278072 CEST	8.8.8.8	192.168.2.4	0xfb1f	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:37.014718056 CEST	8.8.8.8	192.168.2.4	0xd864	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:42.740317106 CEST	8.8.8.8	192.168.2.4	0xb4f7	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:48.351994038 CEST	8.8.8.8	192.168.2.4	0x8a93	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:53.970079899 CEST	8.8.8.8	192.168.2.4	0xbb18	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:00:59.499267101 CEST	8.8.8.8	192.168.2.4	0x6dbc	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:01:05.269151926 CEST	8.8.8.8	192.168.2.4	0xd178	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:01:10.789726973 CEST	8.8.8.8	192.168.2.4	0x74e6	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)
Jun 11, 2021 15:01:16.041094065 CEST	8.8.8.8	192.168.2.4	0xbc5c	No error (0)	kjjuigfdul lygigyftku yluylygily fidyyuljhd .ydns.eu		185.140.53.135	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ORDER.exe PID: 6952 Parent PID: 5896

General

Start time:	14:59:05
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER.exe'
Imagebase:	0x470000
File size:	536064 bytes
MD5 hash:	425F6B1E9437B1F1DB352D1393D236D5
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: 00000001.00000002.733532456.0000000003B71000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.733532456.0000000003B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.733532456.0000000003B71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.733930181.0000000003D27000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.733930181.0000000003D27000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.733930181.0000000003D27000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6920 Parent PID: 6952

General

Start time:	14:59:45
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\Odstcl' /XML 'C:\Users\user\AppData\Local\Temp\tmp6A1C.tmp'
Imagebase:	0x340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6936 Parent PID: 6920

General

Start time:	14:59:46
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ORDER.exe PID: 7148 Parent PID: 6952

General

Start time:	14:59:46
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x690000
File size:	536064 bytes
MD5 hash:	425F6B1E9437B1F1DB352D1393D236D5
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.00000002.906988359.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.906988359.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.906988359.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.909542100.0000000003D17000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.909542100.0000000003D17000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.728181195.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.728181195.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.728181195.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.910722949.0000000005600000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.910722949.0000000005600000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.728520571.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.728520571.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.728520571.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.911027683.00000000059C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.911027683.00000000059C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.911027683.00000000059C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4388 Parent PID: 7148

General

Start time:	14:59:48
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp777A.tmp'
Imagebase:	0x340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6840 Parent PID: 4388

General

Start time:	14:59:49
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ORDER.exe PID: 6044 Parent PID: 968

General

Start time:	14:59:50
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ORDER.exe 0
Imagebase:	0x590000
File size:	536064 bytes
MD5 hash:	425F6B1E9437B1F1DB352D1393D236D5
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: 00000010.00000002.815063432.0000000003D01000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.815063432.0000000003D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.815063432.0000000003D01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 7116 Parent PID: 6044

General

Start time:	15:00:23
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\Odstcl' /XML 'C:\Users\user\AppData\Local\Temp\tmpFE00.tmp'
Imagebase:	0x340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4552 Parent PID: 7116

General

Start time:	15:00:24
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ORDER.exe PID: 4480 Parent PID: 6044

General

Start time:	15:00:24
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x550000
File size:	536064 bytes
MD5 hash:	425F6B1E9437B1F1DB352D1393D236D5
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: 00000018.00000000.809591547.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000000.809591547.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000000.809591547.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000000.810011437.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000000.810011437.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000000.810011437.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.824635528.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.824635528.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.824635528.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.826135770.0000000002B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.826135770.0000000002B71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.826223724.0000000003B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.826223724.0000000003B71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis