ID: 433519
Sample Name: Invoice#06-11-2021_PDF.vbs
Cookbook: default.jbs
Time: 08:07:21
Date: 12/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

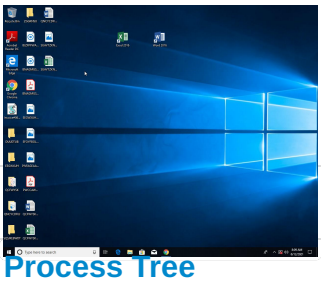
Analysis Report Invoice#06-11-2021_PDF.vbs

Overview

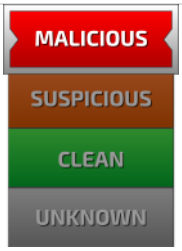
General Information

Sample Name:	Invoice#06-11-2021_PDF.vbs
Analysis ID:	433519
MD5:	fcc6014f7ee0539..
SHA1:	2f006d44ad82ca7.
SHA256:	699d670809bccd..
Tags:	NanoCore RAT vbs
Infos:	

Most interesting Screenshot:



Detection



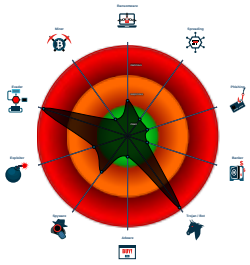
Nanocore AgentTesla

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

Signatures

- Benign windows process drops PE f…
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- VBScript performs obfuscated calls …
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 4804 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice#06-11-2021_PDF.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - file1.exe (PID: 5784 cmdline: 'C:\Users\user\AppData\Local\Temp\file1.exe' MD5: 07C82C84BAEC92953A270419C72D7F10)
    - schtasks.exe (PID: 5412 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HHyKJahmIz' /XML 'C:\Users\user\AppData\Local\Temp\tmpC46.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - file1.exe (PID: 4076 cmdline: {path} MD5: 07C82C84BAEC92953A270419C72D7F10)
  - 2name.exe (PID: 5828 cmdline: 'C:\Users\user\AppData\Local\Temp\2name.exe' MD5: CF4CD927CCC626FB016D0E91CF6BD456)
    - 2name.exe (PID: 5004 cmdline: {path} MD5: CF4CD927CCC626FB016D0E91CF6BD456)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c687c38e-2b2d-4d96-b5eb-9a31ccba",
  "Group": "Sys",
  "Domain1": "sys2021.linkpc.net",
  "Domain2": "",
  "Port": 11940,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "result@jetport-aero.comNiniola@456mail.jetport-aero.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.479174515.000000000433 4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000015.00000000.291952352.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000015.00000000.291952352.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000015.00000000.291952352.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000015.00000002.468642288.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 37 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
21.2.file1.exe.4346f00.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
21.2.file1.exe.4346f00.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
21.2.file1.exe.4346f00.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
21.2.file1.exe.5680000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
21.2.file1.exe.5680000.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 48 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

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

.NET source code contains very large strings

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.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

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

Yara detected AgentTesla

Yara detected AgentTesla

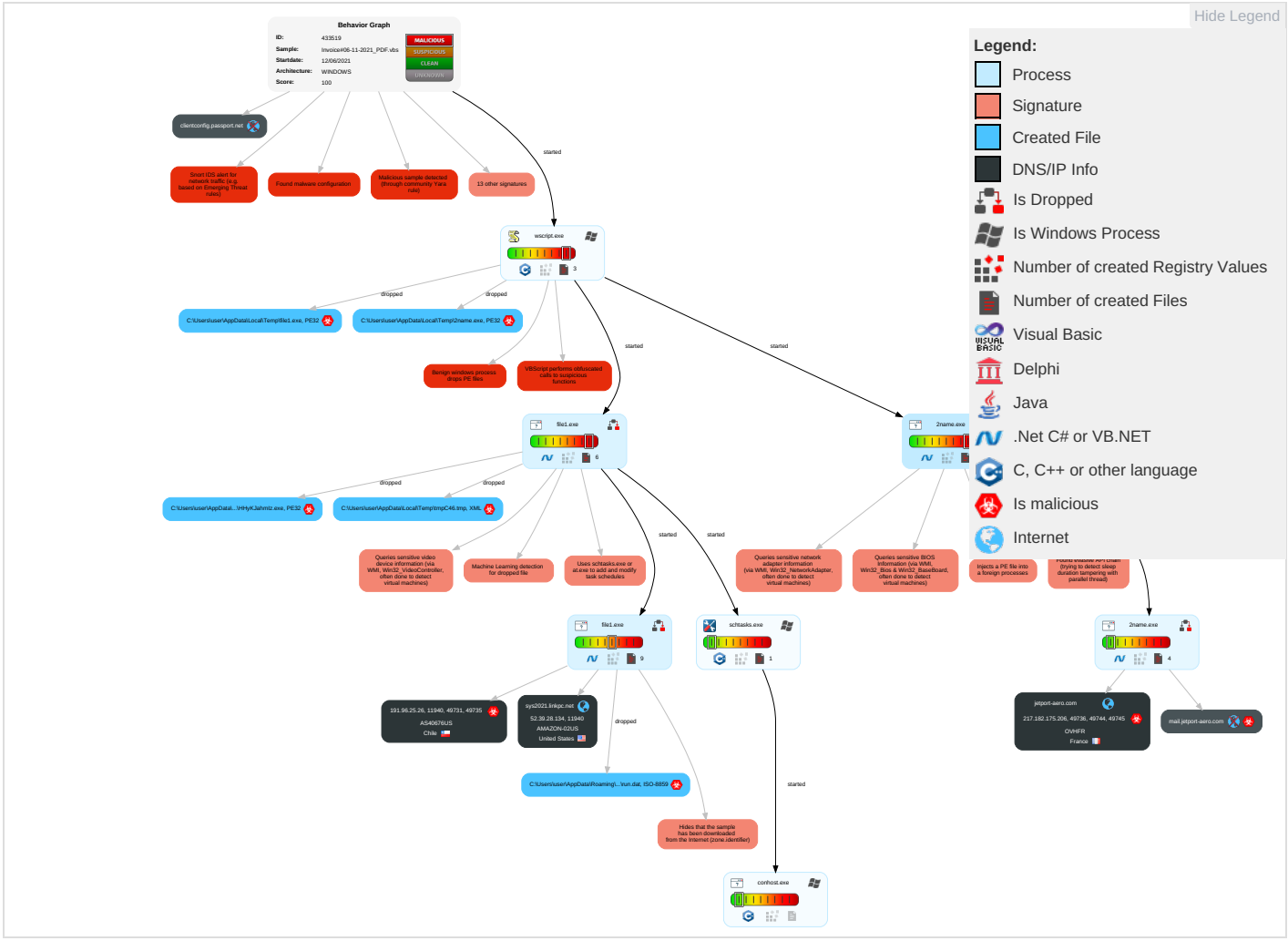
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 3 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Default Accounts	Scripting 1 2 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 1	Logon Script (Windows)	Process Injection 1 1 2	Scripting 1 2 1	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Network Logon Script	Software Packing 2 2	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Virtualization/Sandbox Evasion 2 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 4 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypte Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 2	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusca Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

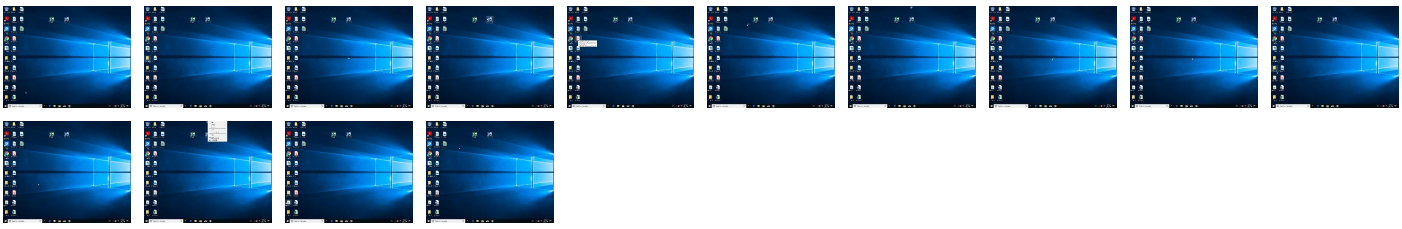
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HHyKJahmIz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\file1.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2name.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.file1.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.file1.exe.4346f00.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
21.0.file1.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.file1.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.2name.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
21.2.file1.exe.5c00000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
16.0.2name.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	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://www.sajatypeworks.com4	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.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.jiyu-kobo.co.jp/Y0/X	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://r3.i.lencr.org/0/	0%	Avira URL Cloud	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.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnk	0%	Avira URL Cloud	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://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://gKSfZA.com	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	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	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	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.galapagosdesign.com/c	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.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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://x1.i.len	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sys2021.linkpc.net	52.39.28.134	true	false		high
jetport-aero.com	217.182.175.206	true	true		unknown
mail.jetport-aero.com	unknown	unknown	true		unknown
clientconfig.passport.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
sys2021.linkpc.net	false		high

URLs from Memory and Binaries

Contacted IPs

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.96.25.26	unknown	Chile		40676	AS40676US	true
52.39.28.134	sys2021.linkpc.net	United States		16509	AMAZON-02US	false
217.182.175.206	jetport-aero.com	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433519
Start date:	12.06.2021
Start time:	08:07:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice#06-11-2021_PDF.vbs
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:	37
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.winVBS@12/8@5/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:08:52	API Interceptor	662x Sleep call for process: file1.exe modified
08:08:56	API Interceptor	658x Sleep call for process: 2name.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
191.96.25.26	Invoice Payment_PDF.vbs	Get hash	malicious	Browse	
	Invoice for B1019855_PDF.vbs	Get hash	malicious	Browse	
	02_extracted.exe	Get hash	malicious	Browse	
	Invoice No B1019855_PDF.vbs	Get hash	malicious	Browse	
	02_extracted.exe	Get hash	malicious	Browse	
	03_extracted.exe	Get hash	malicious	Browse	
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	
	Spec_PDF.vbs	Get hash	malicious	Browse	
	SpecPDF.vbs	Get hash	malicious	Browse	
52.39.28.134	02_extracted.exe	Get hash	malicious	Browse	
217.182.175.206	Invoice Payment_PDF.vbs	Get hash	malicious	Browse	
	Invoice for B1019855_PDF.vbs	Get hash	malicious	Browse	
	01_extracted.exe	Get hash	malicious	Browse	
	Invoice No B1019855_PDF.vbs	Get hash	malicious	Browse	
	9e7d034c_by_Libranalysis.xlsm	Get hash	malicious	Browse	
	SecuriteInfo.com.VB.Trojan.Valyria.4579.10155.xlsm	Get hash	malicious	Browse	
	SecuriteInfo.com.VB.Trojan.Valyria.4579.10155.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sys2021.linkpc.net	Invoice Payment_PDF.vbs	Get hash	malicious	Browse	• 51.178.229.162
	Invoice for B1019855_PDF.vbs	Get hash	malicious	Browse	• 51.178.229.162
	02_extracted.exe	Get hash	malicious	Browse	• 52.39.28.134
	Invoice No B1019855_PDF.vbs	Get hash	malicious	Browse	• 51.210.201.99
	01_extracted.exe	Get hash	malicious	Browse	• 46.105.77.230
	02_extracted.exe	Get hash	malicious	Browse	• 46.105.77.230
	02_extracted.exe	Get hash	malicious	Browse	• 79.137.109.121
	03_extracted.exe	Get hash	malicious	Browse	• 79.137.109.121
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 87.98.245.48
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 79.137.109.121
	Spec_PDF.vbs	Get hash	malicious	Browse	• 105.112.11.245
	SpecPDF.vbs	Get hash	malicious	Browse	• 179.43.166.32

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	JHSkaPIXXA.exe	Get hash	malicious	Browse	• 51.254.187.177
	CBI8Rv3xZ7.dll	Get hash	malicious	Browse	• 51.77.82.110
	hcTYYoyYOS.dll	Get hash	malicious	Browse	• 51.77.82.110
	CBI8Rv3xZ7.dll	Get hash	malicious	Browse	• 51.77.82.110
	hcTYYoyYOS.dll	Get hash	malicious	Browse	• 51.77.82.110
	Purchase_Order.exe	Get hash	malicious	Browse	• 213.186.33.5
	ORDER-21611docx.exe	Get hash	malicious	Browse	• 87.98.245.48
	s6ljEIsdF3.exe	Get hash	malicious	Browse	• 176.31.95.228
	hb5swSGLBT.exe	Get hash	malicious	Browse	• 176.31.95.228
	CM0Q30sK3K.exe	Get hash	malicious	Browse	• 176.31.95.228
	zIrx1wUddJ.exe	Get hash	malicious	Browse	• 144.217.14.109
	8qdfmqz1PN.exe	Get hash	malicious	Browse	• 51.222.56.151
	New Order PO2193570O1.doc	Get hash	malicious	Browse	• 51.222.56.151
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	• 51.222.56.151
	Request For Quote.exe	Get hash	malicious	Browse	• 158.69.138.23
	payload.html	Get hash	malicious	Browse	• 145.239.131.60
	6VYNUalwUt.exe	Get hash	malicious	Browse	• 178.33.222.241
	New Inquiry.exe	Get hash	malicious	Browse	• 158.69.138.23
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	• 51.222.56.151
	Requestforquote.exe	Get hash	malicious	Browse	• 158.69.138.23
AMAZON-02US	CIGi9PIHbu.exe	Get hash	malicious	Browse	• 3.18.3.168

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	research-1234799369.xlsb	Get hash	malicious	Browse	• 52.220.160.98
	microsoft office 2007 service pack 2.exe	Get hash	malicious	Browse	• 13.248.148.254
	ws8W4yPAvg.exe	Get hash	malicious	Browse	• 3.22.15.135
	UOMp9cDcqZ.exe	Get hash	malicious	Browse	• 52.58.78.16
	OrderKLB210568.exe	Get hash	malicious	Browse	• 34.215.126.147
	q7jxy6gZMb.exe	Get hash	malicious	Browse	• 104.192.141.1
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 52.219.158.14
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 52.17.153.103
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 13.224.195.88
	ehDnx4Ke5d.exe	Get hash	malicious	Browse	• 3.22.15.135
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 3.34.12.41
	c71fd2gJus.exe	Get hash	malicious	Browse	• 52.219.64.3
	XQehPgTn35.exe	Get hash	malicious	Browse	• 3.136.65.236
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
AS40676US	ITAPQJikGw.exe	Get hash	malicious	Browse	• 172.107.55.6
	KI91QtYDef.exe	Get hash	malicious	Browse	• 104.217.8.109
	quotation zip.exe	Get hash	malicious	Browse	• 185.215.224.53
	template-jn02b3.dot	Get hash	malicious	Browse	• 207.231.106.130
	y31Lwif2sE.lnk	Get hash	malicious	Browse	• 45.61.138.207
	MJH.exe	Get hash	malicious	Browse	• 46.243.207.43
	Swift copy_9808.exe	Get hash	malicious	Browse	• 104.217.141.243
	Document_46161561.xls	Get hash	malicious	Browse	• 107.160.244.54
	ICNdIx3GY1.exe	Get hash	malicious	Browse	• 104.217.8.122
	SecuriteInfo.com.WinGo.GoCLR.A.24820.exe	Get hash	malicious	Browse	• 45.61.136.223
	cb5b3ec1be5f432cec70fbea8d525210ef25570b56fba.exe	Get hash	malicious	Browse	• 104.217.8.122
	1VdxXmBPdY.exe	Get hash	malicious	Browse	• 104.217.8.122
	62lNIwplP8.exe	Get hash	malicious	Browse	• 45.61.136.223
	iBpCEHz2q4.exe	Get hash	malicious	Browse	• 104.217.8.122
	Invoice Payment_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	Y8bZnrFXSo.exe	Get hash	malicious	Browse	• 104.217.8.122
	ZqdsbHIY5d.exe	Get hash	malicious	Browse	• 104.217.8.122
	wfIHlX06iC.exe	Get hash	malicious	Browse	• 104.217.8.122
	ftl1MRlCZu.exe	Get hash	malicious	Browse	• 104.217.8.122
	Fki4Q91Cvm.exe	Get hash	malicious	Browse	• 104.217.8.122

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\2name.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\2name.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9t0U2WUXBQav:MLF20NaL329hJ5g522rWz2p29XBT
MD5:	2703120C370FBB4A8BA08C6D1754039E
SHA1:	EC0DB47BF00A4A828F796147619386C0BBEA66A1

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\2name.exe.log	
SHA-256:	F95566974BC44F3A757CAFB1456D185D8F333AC84775089DE18310B90C18B1BC
SHA-512:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192EE 48
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de9980 4c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\file1.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\file1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9t0U2WUXBQav:MLF20NaL329hJ5g522rWz2p29XBT
MD5:	2703120C370FBB4A8BA08C6D1754039E
SHA1:	EC0DB47BF00A4A828F796147619386C0BBEA66A1
SHA-256:	F95566974BC44F3A757CAFB1456D185D8F333AC84775089DE18310B90C18B1BC
SHA-512:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192EE 48
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de9980 4c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Temp\2name.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	726016
Entropy (8bit):	7.460683048230593
Encrypted:	false
SSDEEP:	12288:s4Vk+Co34f3xqyPOdN7CEd6ytjAzYhoWtaGiVXRwO:sUCo34gyWdN7H6SDzAjJRwO
MD5:	CF4CD927CCC626FB016D0E91CF6BD456
SHA1:	16C9EA9C6050EC976537ADE42C5C049F7AF2599B
SHA-256:	03D512E79C0748CC83D5BCB4B8847534D7E81D929DAB496727ACBEEC1A5FD694
SHA-512:	422F85A2D020E87D9936668C3D4863C49503FD62070BD6A80B5334FBAA77A55C4095FB53AAB2015498133FAD3FF65CC98090A6C012D9B2F325702016BB51D215
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....(... ...@....@.. ..... ..@.....p(..O....@.....`.....8'..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(.....H.....D...,).....p,.....r...p}.....}.....(.....(.....*..0.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{....o....r[..p(....-..{....o....r[..p(....+.....,.r]..p(....&+.**...(.....*..*...0..+.....,..{.....+.....,..{....o.....(.....*..0..N.....(....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}. ....s....}.....s....}.....s....}.....s....}.....s....}.....s

C:\Users\user\AppData\Local\Temp\file1.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	756224
Entropy (8bit):	7.493608714130465
Encrypted:	false
SSDEEP:	12288:S42kl8+drZTnwWp/OdrFYU+8hs3pVo1f9majwN9DLHvBYWSsVWSy:SY8+drZrp2d6P3pVo1vydrvBYeV9
MD5:	07C82C84BAEC92953A270419C72D7F10
SHA1:	DB68FCB828195BC4556E8A4725BA1BF5057A7C56
SHA-256:	074EE7EF8958EA94C8E5B35D87DAE1B8CFBA9FAF46FB15D61C740FBFD600D758
SHA-512:	C70D0AE16A4BDF285DF963B3E80A0737DD7AD9D5B5A82EFFCBA5CF274E1CC96C3B2607D1AFE26AB8E86788C0FA5E7AE903743D70EDDA7F2DFE8EA8DCCEF E5F2F

C:\Users\user\AppData\Local\Temp\file1.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..`.....0..... .....@.. ..... .@.....O.....`..... ....H.....text....~... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....D...4).....x,...p.....r...p}.....}.....(.....(.....*..0.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{ ....o....r[..p(....-..{....o....r[..p(....+....,..r]..p(....&+.**...(.....*..*...0..+.....,..{.....+....,..{....o.....(.....*..0..N.....(....s.....s...}.....s...}.....s...}.....s...}.....s...}.....s...}.. ...s....}.....s....}.....s....}.....s....}.....s

C:\Users\user\AppData\Local\Temp\tmpC46.tmp	
Process:	C:\Users\user\AppData\Local\Temp\file1.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.193758749843159
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBgtn:cbh47TlNQ//rydbz9l3YODOLNdq3c
MD5:	65835A3FDB40FADC683FF7C737DD45B8
SHA1:	B4F8BAC9E41E723EB171ABC7395CC19A318BE781
SHA-256:	5732AC8EE9ECD64FAE6A998D5BBEB68E9B06309DE048562B5394AAAF49131B76
SHA-512:	18A61873F4520F2C61A1289C23797D9DD5BFC4481E4F89016AC77981FA3DA6D90DAF821DB2154607B9444DF3D15919E442798DB15F5A2DB5F8B921928D51D97E
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\file1.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	12:X4LEnybgCF0uCYKZr+dLEnybgCF0uCYKZr+dLEnybgCF0uCYKZr+K:IQnybgC4jh+dQnybgC4jh+dQnybgC4jp
MD5:	AF6AA7C823112E2342E8D98BE5EDE0A9
SHA1:	D48CA92F4FA11CC9619185563F2D57A6099D21D0
SHA-256:	8D2ACD0CB78A2C690E2DCA1E9C92D273DAF4804DF0B4AC55E14D120C96F7671D
SHA-512:	B822403E85339F4FF2D88608D73DA75A149756FF44454386E1EB2451A6CCCE0F65ECA596F95BBBAD942C963F8C4CA2ADE582D6E50750596DB263BA879FB3ECE 1
Malicious:	false
Reputation:	low
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.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\file1.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:bs8t:5t
MD5:	40198B97616273D9646AB6202B43D7C2
SHA1:	873C0C9A032CA79138FEE4AC197D6C360185D6BC
SHA-256:	43F580A134F143DE82F8BA52CEB9736322D918D3C987B56643DC64308B992B6A
SHA-512:	2CB67B647EA406E4E68BDE03B742CEE25CF88B27EB3D9610B5666B836D4BD4579D5D7FB9F4BB41FBB9751F56D0F4405C4A625ADA36E72D6447ED9F73C09309 A
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Preview:	6."..-.H

C:\Users\user\AppData\Roaming\HHyKJahmIz.exe	
Process:	C:\Users\user\AppData\Local\Temp\file1.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	756224
Entropy (8bit):	7.493608714130465
Encrypted:	false
SSDEEP:	12288:S42kl8+drZTnwWp/OdrFYU+8hs3pVo1f9majwN9DLHvBYWSsVWSy:SY8+drZrp2d6P3pVo1vydrvBYeV9
MD5:	07C82C84BAEC92953A270419C72D7F10
SHA1:	DB68FCB828195BC4556E8A4725BA1BF5057A7C56
SHA-256:	074EE7EF8958EA94C8E5B35D87DAE1B8CFBA9FAF46FB15D61C740FBFD600D758
SHA-512:	C70D0AE16A4BDF285DF963B3E80A0737DD7AD9D5B5A82EFFCBA5CF274E1CC96C3B2607D1AFE26AB8E86788C0FA5E7AE903743D70EDDA7F2DFE8EA8DCCEFE5F2F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..`.....0..... .....@.. ..... .@.....O..... ..... ..H.....text....~... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....D...4).....x,...p.....r...p}.....}.....(.....(.....*..0.....{....o....r[..p(....-\.{....o....r[..p(....-E.{....o....r[..p(....-..{ ....o....r[..p(....-..{....o....r[..p(....+....,..r]..p(....&+.**...(....*..*...0..+.....,..{.....+....,..{....o.....(....*..0..N.....(....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.. ...s....}.....s....}.....s....}.....s....}.....s

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.799622098272767
TrID:	• Visual Basic Script (13500/0) 87.10% • Disk Image (Macintosh), GPT (2000/0) 12.90%
File name:	Invoice#06-11-2021_PDF.vbs
File size:	2064477
MD5:	fcc6014f7ee0539aead5f38b4fe5245e
SHA1:	2f006d44ad82ca71319a5bf615677016ff7e918b
SHA256:	699d670809bccdbbdb2ae85d80be86d6fd00586c56e0375df34527d4ec6045cf
SHA512:	a9dd70d2b62ca41c9704379d57011a71cb661e9d8260cce95226f7dc357a91b59f3f99f6cd6d2d6563aaaa05cb84cf3c0284e3e1de72001eb9d6ab816e4fe208
SSDEEP:	24576:Xb14lK6ARrnCSZv3nc/4Y6FmALwmZz2nI/lks167U29/nwGNEaRr8I+TaCinTtKl:HrFm0wfIdkv7KGtmwkDtKW
File Content Preview:	on error resume next..Dim oJKUEaQXRjwWohJKfxRBprCcdayyKzcHoIONamdeSvgNYPTakLyerbyxGiqdcSNSHohfTwksTmitKpDOGYNzAxPNKQGsvzCziOGjhoGobFLFsEmRfcXDFNSJYUVCqsxTkjLwiTgSRZYumKUFdoMTcyuUwwKMSDxjIrUJsqjLvFlfpXWOAQYBfermorAllTzObplvqKMnFBXW..'MOeYawMCewDezhUBqxCcFX

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/12/21-08:09:51.251566	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	11940	192.168.2.3	191.96.25.26
06/12/21-08:09:57.374510	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	11940	192.168.2.3	191.96.25.26
06/12/21-08:10:03.567163	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	11940	192.168.2.3	191.96.25.26
06/12/21-08:10:09.685092	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	11940	192.168.2.3	191.96.25.26
06/12/21-08:10:20.008499	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	11940	192.168.2.3	191.96.25.26

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 12, 2021 08:08:28.403188944 CEST	192.168.2.3	8.8.8.8	0xae51	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Jun 12, 2021 08:08:54.326776028 CEST	192.168.2.3	8.8.8.8	0xdd02	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jun 12, 2021 08:09:15.375874996 CEST	192.168.2.3	8.8.8.8	0xc79a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jun 12, 2021 08:09:33.977591038 CEST	192.168.2.3	8.8.8.8	0x2ccc	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jun 12, 2021 08:09:57.715130091 CEST	192.168.2.3	8.8.8.8	0xb4ee	Standard query (0)	mail.jetport-aero.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 12, 2021 08:08:25.470307112 CEST	8.8.8.8	192.168.2.3	0x5e14	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 12, 2021 08:08:28.467664003 CEST	8.8.8.8	192.168.2.3	0xae51	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Jun 12, 2021 08:08:54.503034115 CEST	8.8.8.8	192.168.2.3	0xdd02	No error (0)	sys2021.linkpc.net		52.39.28.134	A (IP address)	IN (0x0001)
Jun 12, 2021 08:09:15.551716089 CEST	8.8.8.8	192.168.2.3	0xc79a	No error (0)	sys2021.linkpc.net		52.39.28.134	A (IP address)	IN (0x0001)
Jun 12, 2021 08:09:34.038955927 CEST	8.8.8.8	192.168.2.3	0x2ccc	No error (0)	sys2021.linkpc.net		52.39.28.134	A (IP address)	IN (0x0001)
Jun 12, 2021 08:09:57.793838978 CEST	8.8.8.8	192.168.2.3	0xb4ee	No error (0)	mail.jetport-aero.com	jetport-aero.com		CNAME (Canonical name)	IN (0x0001)
Jun 12, 2021 08:09:57.793838978 CEST	8.8.8.8	192.168.2.3	0xb4ee	No error (0)	jetport-aero.com		217.182.175.206	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 12, 2021 08:09:58.023027897 CEST	587	49736	217.182.175.206	192.168.2.3	220-ns3819423.ip-217-182-175.eu ESMTP Exim 4.93 #2 Sat, 12 Jun 2021 11:39:58 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 12, 2021 08:09:58.027066946 CEST	49736	587	192.168.2.3	217.182.175.206	EHLO 639509

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 12, 2021 08:09:58.078576088 CEST	587	49736	217.182.175.206	192.168.2.3	250-ns3819423.ip-217-182-175.eu Hello 639509 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 12, 2021 08:09:58.079933882 CEST	49736	587	192.168.2.3	217.182.175.206	STARTTLS
Jun 12, 2021 08:09:58.133795977 CEST	587	49736	217.182.175.206	192.168.2.3	220 TLS go ahead
Jun 12, 2021 08:09:58.883198977 CEST	587	49736	217.182.175.206	192.168.2.3	421 Lost incoming connection
Jun 12, 2021 08:10:14.266299009 CEST	587	49744	217.182.175.206	192.168.2.3	220-ns3819423.ip-217-182-175.eu ESMTP Exim 4.93 #2 Sat, 12 Jun 2021 11:40:14 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 12, 2021 08:10:14.267148972 CEST	49744	587	192.168.2.3	217.182.175.206	EHLO 639509
Jun 12, 2021 08:10:14.320889950 CEST	587	49744	217.182.175.206	192.168.2.3	250-ns3819423.ip-217-182-175.eu Hello 639509 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 12, 2021 08:10:14.323684931 CEST	49744	587	192.168.2.3	217.182.175.206	STARTTLS
Jun 12, 2021 08:10:14.379235983 CEST	587	49744	217.182.175.206	192.168.2.3	220 TLS go ahead
Jun 12, 2021 08:10:17.940721035 CEST	587	49744	217.182.175.206	192.168.2.3	421 ns3819423.ip-217-182-175.eu lost input connection
Jun 12, 2021 08:10:18.012880087 CEST	587	49745	217.182.175.206	192.168.2.3	220-ns3819423.ip-217-182-175.eu ESMTP Exim 4.93 #2 Sat, 12 Jun 2021 11:40:18 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 12, 2021 08:10:18.013842106 CEST	49745	587	192.168.2.3	217.182.175.206	EHLO 639509
Jun 12, 2021 08:10:18.072870970 CEST	587	49745	217.182.175.206	192.168.2.3	250-ns3819423.ip-217-182-175.eu Hello 639509 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 12, 2021 08:10:18.073750973 CEST	49745	587	192.168.2.3	217.182.175.206	STARTTLS
Jun 12, 2021 08:10:18.127690077 CEST	587	49745	217.182.175.206	192.168.2.3	220 TLS go ahead
Jun 12, 2021 08:10:18.884313107 CEST	587	49745	217.182.175.206	192.168.2.3	421 ns3819423.ip-217-182-175.eu lost input connection
Jun 12, 2021 08:10:18.944071054 CEST	587	49746	217.182.175.206	192.168.2.3	220-ns3819423.ip-217-182-175.eu ESMTP Exim 4.93 #2 Sat, 12 Jun 2021 11:40:18 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 12, 2021 08:10:18.944447041 CEST	49746	587	192.168.2.3	217.182.175.206	EHLO 639509
Jun 12, 2021 08:10:18.995879889 CEST	587	49746	217.182.175.206	192.168.2.3	250-ns3819423.ip-217-182-175.eu Hello 639509 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 12, 2021 08:10:18.996215105 CEST	49746	587	192.168.2.3	217.182.175.206	STARTTLS
Jun 12, 2021 08:10:19.050832033 CEST	587	49746	217.182.175.206	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 4804 Parent PID: 3388

General

Start time:	08:08:06
Start date:	12/06/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice#06-11-2021_PDF.vbs'
Imagebase:	0x7ff679cd0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: file1.exe PID: 5784 Parent PID: 4804

General

Start time:	08:08:10
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Local\Temp\file1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\file1.exe'
Imagebase:	0x5d0000
File size:	756224 bytes
MD5 hash:	07C82C84BAEC92953A270419C72D7F10
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: 00000001.00000002.297937965.0000000003F51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.297937965.0000000003F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.297937965.0000000003F51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.307230936.000000000D351000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.307230936.000000000D351000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.307230936.000000000D351000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 2name.exe PID: 5828 Parent PID: 4804

General

Start time:	08:08:10
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Local\Temp\2name.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\2name.exe'
Imagebase:	0x190000
File size:	726016 bytes
MD5 hash:	CF4CD927CCC626FB016D0E91CF6BD456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.311010210.000000000CDE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.311010210.000000000CDE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.294907318.00000000038B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.294907318.00000000038B1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 2name.exe PID: 5004 Parent PID: 5828

General

Start time:	08:08:47
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Local\Temp\2name.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa30000
File size:	726016 bytes
MD5 hash:	CF4CD927CCC626FB016D0E91CF6BD456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.468518858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.468518858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.477741518.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.477741518.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.288308557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.288308557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: schtasks.exe PID: 5412 Parent PID: 5784

General

Start time:	08:08:48
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HHyKJahmIz' /XML 'C:\Users\user\AppData\Local\Temp\tmpC46.tmp'
Imagebase:	0x930000
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: 5076 Parent PID: 5412

General

Start time:	08:08:49
Start date:	12/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: file1.exe PID: 4076 Parent PID: 5784

General

Start time:	08:08:49
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Local\Temp\file1.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc40000
File size:	756224 bytes
MD5 hash:	07C82C84BAEC92953A270419C72D7F10
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: 00000015.00000002.479174515.0000000004334000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.291952352.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.291952352.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.291952352.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.468642288.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.468642288.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.468642288.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.479905732.0000000005680000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.479905732.0000000005680000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.292645242.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.292645242.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.292645242.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.480599769.0000000005C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.480599769.0000000005C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.480599769.0000000005C00000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis