ID: 411334
Sample Name: Invoice No F1019855_PDF.vbs
Cookbook: default.jbs
Time: 20:00:27
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

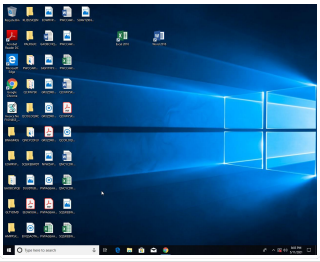
Analysis Report Invoice No F1019855_PDF.vbs

Overview

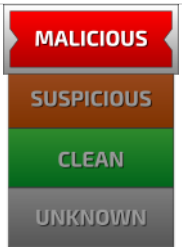
General Information

Sample Name:	Invoice No F1019855_PDF.vbs
Analysis ID:	411334
MD5:	fcf52f96d96c687…
SHA1:	ca29113b7607ec..
SHA256:	fbc5a1e5f8a02c6..
Tags:	NanoCore RAT vbs
Infos:	

Most interesting Screenshot:



Detection



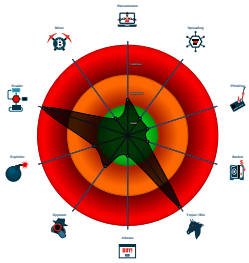
Nanocore AsyncRAT

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 …
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- VBScript performs obfuscated calls …
- Yara detected AntiVM3
- Yara detected AsyncRAT
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Connects to many ports of the same…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 6380 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice No F1019855_PDF.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - file.exe (PID: 6588 cmdline: 'C:\Users\user\AppData\Local\Temp\file.exe' MD5: E6A6EB2982AB17BBB7083493805823BA)
    - schtasks.exe (PID: 7072 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JkeJLChUI' /XML 'C:\Users\user\AppData\Local\Temp\tmpAD9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - file.exe (PID: 7156 cmdline: {path} MD5: E6A6EB2982AB17BBB7083493805823BA)
  - name.exe (PID: 6612 cmdline: 'C:\Users\user\AppData\Local\Temp\name.exe' MD5: 43C4F163196FF02E7AA8C5040375FDA4)
    - schtasks.exe (PID: 7088 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LiydYED' /XML 'C:\Users\user\AppData\Local\Temp\tmpC12.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - name.exe (PID: 800 cmdline: {path} MD5: 43C4F163196FF02E7AA8C5040375FDA4)
- **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"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.255078777.00000000030F1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.256966112.00000000040F9000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000B.00000002.477861276.0000000005590000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0000000B.00000002.477861276.0000000005590000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0000000B.00000002.476715022.0000000004087000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.name.exe.5950000.11.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
11.2.name.exe.5950000.11.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
11.2.name.exe.5950000.11.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
4.2.name.exe.47d8c38.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4.2.name.exe.47d8c38.1.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

Click to see the 43 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

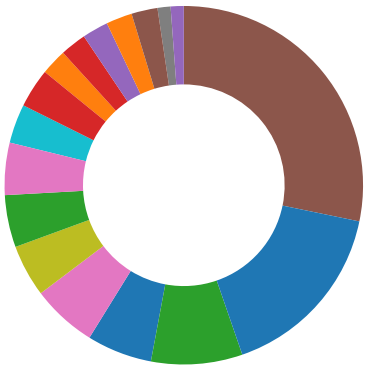
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

Connects to many ports of the same IP (likely port scanning)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

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

Yara detected AsyncRAT

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

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

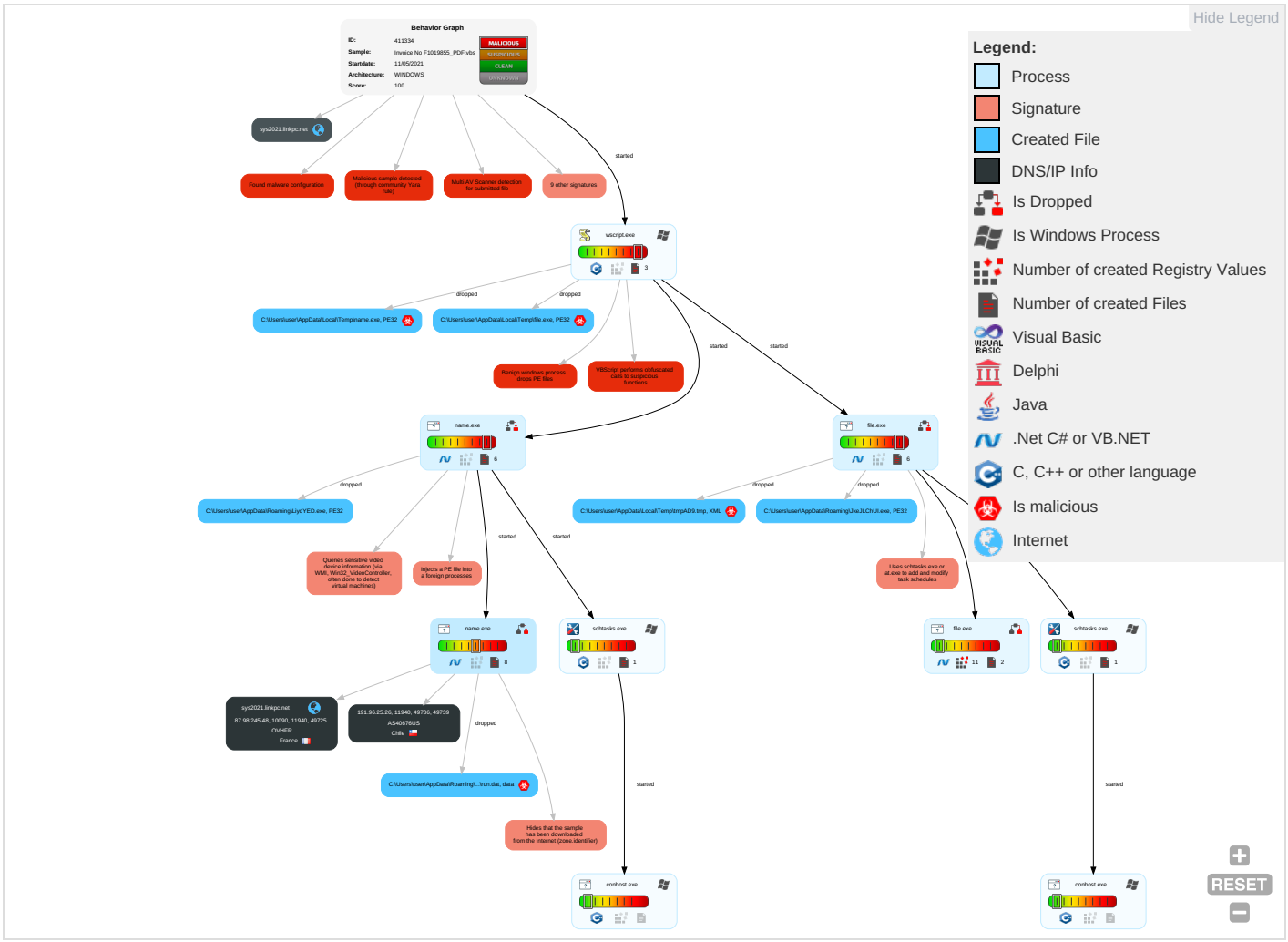
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	E C
Default Accounts	Scripting 1 2 1	Windows Service 2	Access Token Manipulation 1	Scripting 1 2 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	N P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Domain Accounts	Exploitation for Client Execution 1	Scheduled Task/Job 2	Windows Service 2	Obfuscated Files or Information 1 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	R S
Local Accounts	Scheduled Task/Job 2	Logon Script (Mac)	Process Injection 1 1 2	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	N A L P
Cloud Accounts	Cron	Network Logon Script	Scheduled Task/Job 2	Timestomp 1	LSA Secrets	Security Software Discovery 2 1 1	SSH	Keylogging	Data Transfer Size Limits	A L P
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	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
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 Encrypted Non-C2 Protocol	W
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/Obfuscated Non-C2 Protocol	Fi P
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	M

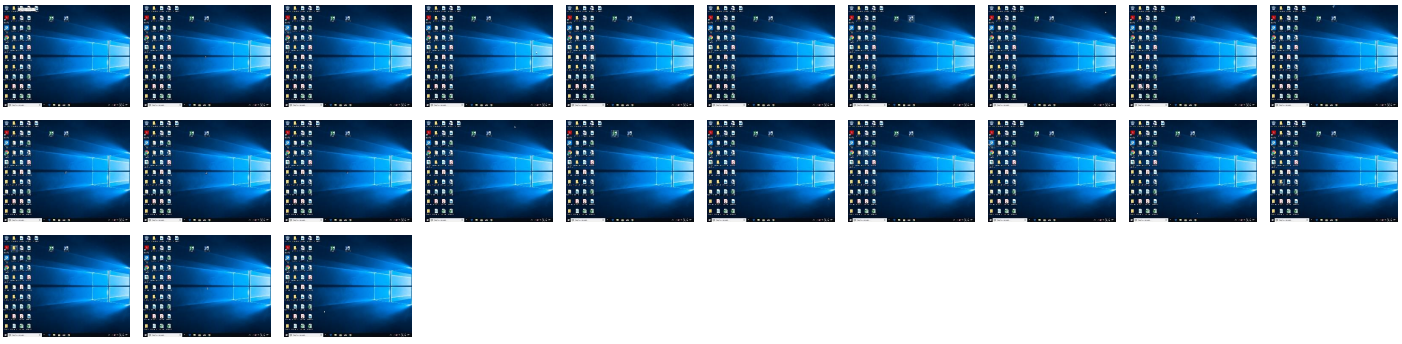
Behavior Graph



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
Invoice No F1019855_PDF.vbs	21%	ReversingLabs	Script-WScript.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.name.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.name.exe.5950000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.2.file.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

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://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.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	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.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.carterandcone.com	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.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	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.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.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.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://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://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comF6	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/rge	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.fonts.comyp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/w	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/i	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	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.carterandcone.comext	0%	Avira URL Cloud	safe	
http://www.fontbureau.com9	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalso	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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.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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	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://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.fonts.comx	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://www.jiyu-kobo.co.jp//sO	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comw	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/u	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sys2021.linkpc.net	87.98.245.48	true	false		high

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high
http://www.founder.com.cn/cn/bThe	file.exe, 00000003.00000002.26 2971462.0000000006170000.00000 002.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high
http://www.tiro.com	name.exe, 00000004.00000002.25 8227103.0000000005A60000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	name.exe, 00000004.00000002.25 8227103.0000000005A60000.00000 002.00000001.sdmp	false		high
http://www.fontbureau.comessed	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	name.exe, 00000004.00000003.21 6797322.000000000597C000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/~	name.exe, 00000004.00000003.21 8188499.0000000005978000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	name.exe, 00000004.00000003.21 4006989.000000000598B000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	file.exe, 00000003.00000002.26 2971462.0000000006170000.00000 002.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	file.exe, 00000003.00000003.22 0798127.0000000006096000.00000 004.00000001.sdmp, file.exe, 0 0000003.00000002.265434370.000 0000007192000.00000004.0000000 1.sdmp, name.exe, 00000004.000 00002.258227103.0000000005A600 00.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF6	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/rge	name.exe, 00000004.00000003.21 8188499.0000000005978000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comlicd	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/4	name.exe, 00000004.00000003.21 8188499.0000000005978000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comyp	name.exe, 00000004.00000003.21 4182404.000000000598B000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/w	file.exe, 00000003.00000003.22 0028378.0000000006096000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/i	name.exe, 00000004.00000003.21 8188499.0000000005978000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/	name.exe, 00000004.00000003.22 0508852.0000000005977000.00000 004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/ana	file.exe, 00000003.00000003.21 7445274.0000000006083000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comext	name.exe, 00000004.00000003.21 6797322.000000000597C000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com9	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalso	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high
http://www.sandoll.co.kr	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/&	name.exe, 00000004.00000003.21 7929078.0000000005977000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	file.exe, 00000003.00000002.26 2971462.0000000006170000.00000 002.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	file.exe, 00000003.00000002.25 5141444.0000000003151000.00000 004.00000001.sdmp	false		high
http://www.sakkal.com	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comx	name.exe, 00000004.00000003.21 4233303.000000000598B000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	file.exe, 00000003.00000003.21 6324625.000000000608E000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high
http://www.fontbureau.com	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, file.exe, 0 0000003.00000003.219359586.000 000000608E000.00000004.0000000 1.sdmp, name.exe, 00000004.000 00002.258227103.0000000005A600 00.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	file.exe, 00000003.00000003.22 0028378.0000000006096000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000003.220508852.000 0000005977000.00000004.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//sO	file.exe, 00000003.00000003.21 7445274.0000000006083000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comw	name.exe, 00000004.00000003.21 4006989.000000000598B000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/L	name.exe, 00000004.00000003.21 7929078.0000000005977000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comion	file.exe, 00000003.00000003.25 3543403.000000000608A000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/u	file.exe, 00000003.00000003.21 7797992.0000000006089000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	file.exe, 00000003.00000003.21 7445274.0000000006083000.00000 004.00000001.sdmp, file.exe, 0 0000003.00000003.217797992.000 0000006089000.00000004.0000000 1.sdmp, name.exe, 00000004.000 00003.217929078.0000000005977000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/w	name.exe, 00000004.00000003.21 7929078.0000000005977000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/?	name.exe, 00000004.00000003.21 7929078.0000000005977000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high
http://www.founder.com.cn/cn	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	name.exe, 00000004.00000003.21 7929078.0000000005977000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/u	file.exe, 00000003.00000003.21 7445274.0000000006083000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	file.exe, 00000003.00000003.21 7445274.0000000006083000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000003.218188499.000 0000005978000.00000004.0000000 1.sdmp, name.exe, 00000004.000 00003.217929078.0000000005977000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	file.exe, 00000003.00000003.25 3543403.000000000608A000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	file.exe, 00000003.00000002.26 5434370.0000000007192000.00000 004.00000001.sdmp, name.exe, 0 0000004.00000002.258227103.000 0000005A60000.00000002.0000000 1.sdmp	false		high
http://www.fontbureau.comalic	file.exe, 00000003.00000003.21 9359586.000000000608E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cntic	file.exe, 00000003.00000003.21 5566337.000000000608E000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.96.25.26	unknown	Chile		40676	AS40676US	false
87.98.245.48	sys2021.linkpc.net	France		16276	OVHFR	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411334
Start date:	11.05.2021
Start time:	20:00:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice No F1019855_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@15/9@24/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.4%) • Quality average: 39.5% • Quality standard deviation: 33.8%
HCA Information:	• Successful, ratio: 97% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.210.154, 168.61.161.212, 104.43.193.48, 92.122.145.220, 40.88.32.150, 23.57.80.111, 92.122.213.247, 92.122.213.194, 8.241.90.126, 8.241.78.126, 8.253.207.120, 67.26.75.254, 8.238.35.254, 51.103.5.186, 20.54.26.129 • Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:01:32	API Interceptor	1x Sleep call for process: file.exe modified
20:01:33	API Interceptor	801x Sleep call for process: name.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
191.96.25.26	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	
	Spec_PDF.vbs	Get hash	malicious	Browse	
	SpecPDF.vbs	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
87.98.245.48	Cotizacin.jar	Get hash	malicious	Browse	
	ORDER-0319.pdf.exe	Get hash	malicious	Browse	
	PO-21322.xlsm	Get hash	malicious	Browse	
	ORDER-21031566AF.exe	Get hash	malicious	Browse	
	Booking Confirmation 02222021951 - copy -PDF.exe	Get hash	malicious	Browse	
	Document.exe	Get hash	malicious	Browse	
	ORDER #0622.exe	Get hash	malicious	Browse	
	hiIXRIdkjB.exe	Get hash	malicious	Browse	
	LIST_OF_IDs.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sys2021.linkpc.net	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
AS40676US	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• 107.160.234.116
	f41e9f9d_by_Libranalysis.exe	Get hash	malicious	Browse	• 107.160.177.197
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	2f50000.exe	Get hash	malicious	Browse	• 38.39.192.78
	PT6-1152.doc	Get hash	malicious	Browse	• 45.61.136.72
	PT6-1152.doc	Get hash	malicious	Browse	• 45.61.136.72
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 104.217.141.249
	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• 107.160.232.135
	Spec_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	8CgG2kY3Ow.dll	Get hash	malicious	Browse	• 45.61.138.153
	DHL_S390201.exe	Get hash	malicious	Browse	• 45.34.249.30
	978463537_BL FOR APPROVAL.doc	Get hash	malicious	Browse	• 45.34.114.71
	SpecPDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	7mB68AZqJs.exe	Get hash	malicious	Browse	• 104.217.143.44
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 172.107.55.6
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• 172.107.55.6
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• 107.160.118.15
	swift note.xlsx	Get hash	malicious	Browse	• 107.160.118.15
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 107.160.118.15
	YPJ9DZYIpO	Get hash	malicious	Browse	• 107.169.29.204
OVHFR	Ujmadjok.exe	Get hash	malicious	Browse	• 51.222.195.7
	Sibco.exe	Get hash	malicious	Browse	• 51.222.195.7
	A1qhcbngFV.exe	Get hash	malicious	Browse	• 51.178.207.67
	eGDBXEE70Awbg6D.exe	Get hash	malicious	Browse	• 66.70.204.222
	94280a43_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.39.198.225
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• 213.186.33.5
	w5FqUzyDmszpdwX.exe	Get hash	malicious	Browse	• 66.70.204.222
	SNBDBM2No4.exe	Get hash	malicious	Browse	• 213.186.33.5
	Garanti BBVA Payment Slip.exe	Get hash	malicious	Browse	• 66.70.204.222
	Purchase Inquiry 11.05.2021.exe	Get hash	malicious	Browse	• 51.79.80.214
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 5.135.185.231
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.195.38.32
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.195.38.32
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.195.38.32
	black	Get hash	malicious	Browse	• 91.121.140.167
	.report_system	Get hash	malicious	Browse	• 94.23.247.226
	98c87992_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.38.220.85

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\name.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\name.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:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192E 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_v4.0_32\UsageLogs\file.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC 2A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0. 0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System. ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyT oken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.C onfiguration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\ 8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C: \Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\file.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	703488
Entropy (8bit):	7.213651737719658
Encrypted:	false
SSDEEP:	12288:doLLoS60/K7yh0K40auRhRwWSEUJu1NMm8kJ:doLApuRmZJu18E
MD5:	E6A6EB2982AB17BBB7083493805823BA
SHA1:	79D317D1F2E41E580CF84942C97C044C97A20A3A
SHA-256:	263EB4034FE9B2BFE0E8472280BAB407EFFA3116391822A7CA34B2C480C438BF

C:\Users\user\AppData\Local\Temp\file.exe

SHA-512:	7A91A5A264D9F28C68562082B85A18B7E1A90235318EA1222C96DDB0656EA1CBC58F47AE8E16CCADA708021011B69DBFB1D0F77B639C79F96903A77D119568E
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...2GZ.....0.....V.... .....@.. ....@.....O..... ....H.....text...\.... ....`.rsrc.....@..@.reloc..... .....@..B.....8.....H.....e...~.....v.....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..2.....($.....(%.....,...("......(&....('...(.....*>...(#...(.....*...0.....b`.+..*...(" ... .(...h..(!...h(....(Q...&*..0.....

C:\Users\user\AppData\Local\Temp\name.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	784896
Entropy (8bit):	7.328703413450174
Encrypted:	false
SSDEEP:	12288:OoLLoS60/K7yh036vCww4Scd3IGj483ESuvkuDKsjLtZTMfLodiMW2G:OoLA3AScdYKSvkItxeUdinh
MD5:	43C4F163196FF02E7AA8C5040375FDA4
SHA1:	F826B410B31CB251DD85F3663735B2F410906517
SHA-256:	A585841F956F17925242996A98836B0D08767DDB179B4B41FD18A5DE719C531C
SHA-512:	264FB4514257080068CEC2915BE6F81EA759812F059B9B969B2F40EE6E502497F22F66C0EFE9B2F5736D6C61F1C7967E9F801B1DF33D100261D4A1B560DDEF7E
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0.....:.... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text...@.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....e..,~.....v...$....).....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(....h}.....(...h }.....(!... .....(V...&*>...("...(.....*..0..C.....(L...&.....(....h}.....(...h}.....(!... .....(V...&*>...("...(.....*..0..2.....(#.....($.....,...(!.....(%....(&...(.....*>...("...(.....*...0..... .....b`.+..*...(!... .....(....h..(...h(....(Q...&*..0.....

C:\Users\user\AppData\Local\Temp\tmpAD9.tmp

Process:	C:\Users\user\AppData\Local\Temp\file.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.192815293348326
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB30tn:cbh47TlNQ//rydbz9I3YODOLNdq3g
MD5:	E6F11A409139683DDF68EF89AA26A7F4
SHA1:	C22B8452571C1B21B6DC42FD934AC5D89F506236
SHA-256:	8DE96994F8D061A076A09392E6ABB30A7FFC1071CD655B47395783E2B1616E2E
SHA-512:	3DD984011B2D39D0CA76C282F4391C94F95ACDA2917BE2C3304C976240F9651408AF8D38D34DDB49ABE3918B852EC69769DD4864DD41C5787A3547C938A3600
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <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\tmpC12.tmp

Process:	C:\Users\user\AppData\Local\Temp\name.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.186918440260069
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBvtn:cbh47TlNQ//rydbz9I3YODOLNdq3D
MD5:	5AAA212919E5C5942B4AF96D5F40E307
SHA1:	B842F7B4B461F442963F87F92EF40C106A6AE72B
SHA-256:	E751A34F0CF72662A8D9CAAA54A22CDB7B344E965A9CFAD36943612343C7EF5E
SHA-512:	7E4B097A289BED9AF862B4B04F4990E1F06B317B7C4CEA70D3B334DB9F2E2D2EB23C0F3192F51149181C87A75D7606FC7008B1DFF82970AE19F117307F7A4518
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpC12.tmp	
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\AppData\Local\Temp\name.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ax8t:68t
MD5:	77A6F2F5CCD6DD1BFCDC998F7A58D479
SHA1:	CFD03C773EF88A3FBCA9018C45311FD7D7770FDB
SHA-256:	3BD10D98336C9729F78D458266C499AF4BDB01A79015E7F4F1B9CEA5C33B1E8E
SHA-512:	EB90A4E934243F430E3EA744052EF22384815F3028E5AEECAF501A700A31A443553BA8FDD99DC18F5C8025E6A367A2A460EB775DA8895012C0FCEF2BD25D38F
Malicious:	**true**
Preview:	.3.C...H

C:\Users\user\AppData\Roaming\JkeJLChUI.exe	
Process:	C:\Users\user\AppData\Local\Temp\file.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	703488
Entropy (8bit):	7.213651737719658
Encrypted:	false
SSDEEP:	12288:doLLoS60/K7yh0K40auRhRwWSEUJu1NMm8kJ:doLApuRmZJu18E
MD5:	E6A6EB2982AB17BBB7083493805823BA
SHA1:	79D317D1F2E41E580CF84942C97C044C97A20A3A
SHA-256:	263EB4034FE9B2BFE0E8472280BAB407EFFA3116391822A7CA34B2C480C438BF
SHA-512:	7A91A5A264D9F28C68562082B85A18B7E1A90235318EA1222C96DDB0656EA1CBC58F47AE8E16CCADA708021011B69DBFB1D0F77B639C79F96903A77D119568E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...2GZ.....0.....V.... .....@.. ....@.....O..... ....H.....text...\.... ....`.rsrc.....@..@.reloc..... .....@..B.....8.....H.....e...~.....v.....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..C.....(L...&.....(...h}.....(!...h}.....("... .....(V...&*>...(#...(.....*..0..2.....($.....(%.....(.....(&....('...(.....*>...(#...(.....*...0.....b`.+..*...(" ... .(...h..(!...h(....(Q...&*..0.....

C:\Users\user\AppData\Roaming\LiydYED.exe	
Process:	C:\Users\user\AppData\Local\Temp\name.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	784896
Entropy (8bit):	7.328703413450174
Encrypted:	false
SSDEEP:	12288:OoLLoS60/K7yh036vCww4Scd3IGj483ESuvkuDKsjLtZTMfLodiMW2G:OoLA3AScdYKSvkItxeUdinh
MD5:	43C4F163196FF02E7AA8C5040375FDA4
SHA1:	F826B410B31CB251DD85F3663735B2F410906517
SHA-256:	A585841F956F17925242996A98836B0D08767DDB179B4B41FD18A5DE719C531C
SHA-512:	264FB4514257080068CEC2915BE6F81EA759812F059B9B969B2F40EE6E502497F22F66C0EFE9B2F5736D6C61F1C7967E9F801B1DF33D100261D4A1B560DDEF7E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0.....:.... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text...@.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....e..,~.....v...$....).....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(....h}.....(...h }.....(!... .....(V...&*>...("...(.....*..0..C.....(L...&.....(....h}.....(...h}.....(!... .....(V...&*>...("...(.....*..0..2.....(#.....($.....(.....(!.....(%....(&...(.....*>...("...(.....*...0..... .....b`.+..*...(!... .....(....h..(...h(....(Q...&*..0.....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.738078637712689
TrID:	• Visual Basic Script (13500/0) 87.10% • Disk Image (Macintosh), GPT (2000/0) 12.90%
File name:	Invoice No F1019855_PDF.vbs
File size:	2072856
MD5:	fcf52f96d96c68788ffe13fcccd4c89c
SHA1:	ca29113b7607ecb7d9a65d8285d7d36f367b1cd0
SHA256:	fbc5a1e5f8a02c644cf207d40885c7973dc7e4809b97f676927da3e13e17ed1f
SHA512:	bf38bab39d1358892b0d7fc65bfd8688078b4404de0edb3231a7c96b0d1df428786c5c8bf07ba07f7b88913a3a1de72d46063df689edc428e3132e8838540bf8
SSDEEP:	24576:b+Ve64mPEkJd1XpdQ5YImc4yFNkVQtJpE5821c5+D5PTxrpWhFcW1Gi/zQSov0FF:blz4ToQsx46J/0
File Content Preview:	on error resume next..Dim RDMsYFgRTjlFiPOXgngfmYrotYHtgshiEaKISfIKcNDgFgGvTPhfBXNsMXzAymkaCCAHEFFAfVCZVKjMRLZRLBhgNSwugIMpdcdDfzqNKgAfUoXBomimNTPBVUumJKUXJNwthfhSVMGfBCLZvvFuZacJNciLEDEAMcWGrdUIEQQANjzTIVrOEZyjlmfFxWNSIGSYfEhR..'bxpIJbwdcPCjMpwmenVFyOLiCy

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:01:41.735663891 CEST	49725	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:42.043533087 CEST	11940	49725	87.98.245.48	192.168.2.3
May 11, 2021 20:01:42.612586021 CEST	49725	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:42.946511984 CEST	11940	49725	87.98.245.48	192.168.2.3
May 11, 2021 20:01:43.612987041 CEST	49725	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:43.841502905 CEST	11940	49725	87.98.245.48	192.168.2.3
May 11, 2021 20:01:49.301887035 CEST	49729	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:49.632344961 CEST	11940	49729	87.98.245.48	192.168.2.3
May 11, 2021 20:01:50.222598076 CEST	49729	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:50.553210020 CEST	11940	49729	87.98.245.48	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:01:51.222748995 CEST	49729	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:51.523634911 CEST	11940	49729	87.98.245.48	192.168.2.3
May 11, 2021 20:01:54.401385069 CEST	49732	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:01:54.673207998 CEST	10090	49732	87.98.245.48	192.168.2.3
May 11, 2021 20:01:55.222990036 CEST	49732	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:01:55.433574915 CEST	10090	49732	87.98.245.48	192.168.2.3
May 11, 2021 20:01:55.743906021 CEST	49733	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:56.019952059 CEST	49732	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:01:56.042218924 CEST	11940	49733	87.98.245.48	192.168.2.3
May 11, 2021 20:01:56.347024918 CEST	10090	49732	87.98.245.48	192.168.2.3
May 11, 2021 20:01:56.613817930 CEST	49733	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:56.864617109 CEST	11940	49733	87.98.245.48	192.168.2.3
May 11, 2021 20:01:57.426366091 CEST	49733	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:01:57.715471983 CEST	11940	49733	87.98.245.48	192.168.2.3
May 11, 2021 20:01:58.201350927 CEST	49734	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:01:58.439827919 CEST	10090	49734	87.98.245.48	192.168.2.3
May 11, 2021 20:01:58.980581045 CEST	49734	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:01.726294041 CEST	49736	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:01.915411949 CEST	11940	49736	191.96.25.26	192.168.2.3
May 11, 2021 20:02:02.426779985 CEST	49736	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:02.615673065 CEST	11940	49736	191.96.25.26	192.168.2.3
May 11, 2021 20:02:03.224565983 CEST	49736	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:03.413295031 CEST	11940	49736	191.96.25.26	192.168.2.3
May 11, 2021 20:02:05.114484072 CEST	49734	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:05.374241114 CEST	10090	49734	87.98.245.48	192.168.2.3
May 11, 2021 20:02:07.429775000 CEST	49739	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:07.618309021 CEST	11940	49739	191.96.25.26	192.168.2.3
May 11, 2021 20:02:08.224159002 CEST	49739	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:08.412794113 CEST	11940	49739	191.96.25.26	192.168.2.3
May 11, 2021 20:02:08.785770893 CEST	49740	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:08.927269936 CEST	49739	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:09.025546074 CEST	10090	49740	87.98.245.48	192.168.2.3
May 11, 2021 20:02:09.118798971 CEST	11940	49739	191.96.25.26	192.168.2.3
May 11, 2021 20:02:09.614939928 CEST	49740	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:09.847903967 CEST	10090	49740	87.98.245.48	192.168.2.3
May 11, 2021 20:02:10.427467108 CEST	49740	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:10.706358910 CEST	10090	49740	87.98.245.48	192.168.2.3
May 11, 2021 20:02:12.841183901 CEST	49741	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:13.165374994 CEST	49742	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:13.275830030 CEST	10090	49741	87.98.245.48	192.168.2.3
May 11, 2021 20:02:13.355648994 CEST	11940	49742	191.96.25.26	192.168.2.3
May 11, 2021 20:02:13.927700996 CEST	49742	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:13.927778959 CEST	49741	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:14.116558075 CEST	11940	49742	191.96.25.26	192.168.2.3
May 11, 2021 20:02:14.227073908 CEST	10090	49741	87.98.245.48	192.168.2.3
May 11, 2021 20:02:14.724626064 CEST	49742	11940	192.168.2.3	191.96.25.26
May 11, 2021 20:02:14.913285017 CEST	11940	49742	191.96.25.26	192.168.2.3
May 11, 2021 20:02:14.927854061 CEST	49741	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:15.149918079 CEST	10090	49741	87.98.245.48	192.168.2.3
May 11, 2021 20:02:17.089134932 CEST	49743	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:17.439536095 CEST	10090	49743	87.98.245.48	192.168.2.3
May 11, 2021 20:02:18.115554094 CEST	49743	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:18.454447031 CEST	10090	49743	87.98.245.48	192.168.2.3
May 11, 2021 20:02:19.076059103 CEST	49743	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:19.098360062 CEST	49747	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:19.323482037 CEST	10090	49743	87.98.245.48	192.168.2.3
May 11, 2021 20:02:19.323514938 CEST	11940	49747	87.98.245.48	192.168.2.3
May 11, 2021 20:02:19.928250074 CEST	49747	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:20.175740004 CEST	11940	49747	87.98.245.48	192.168.2.3
May 11, 2021 20:02:20.725198984 CEST	49747	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:20.938369036 CEST	11940	49747	87.98.245.48	192.168.2.3
May 11, 2021 20:02:24.276612043 CEST	49748	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:24.593111992 CEST	10090	49748	87.98.245.48	192.168.2.3
May 11, 2021 20:02:25.084472895 CEST	49749	11940	192.168.2.3	87.98.245.48

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:02:25.225553036 CEST	49748	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:25.354984045 CEST	11940	49749	87.98.245.48	192.168.2.3
May 11, 2021 20:02:25.508436918 CEST	10090	49748	87.98.245.48	192.168.2.3
May 11, 2021 20:02:25.928728104 CEST	49749	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:26.116236925 CEST	49748	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:26.236618996 CEST	11940	49749	87.98.245.48	192.168.2.3
May 11, 2021 20:02:26.417285919 CEST	10090	49748	87.98.245.48	192.168.2.3
May 11, 2021 20:02:26.944396973 CEST	49749	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:27.213268995 CEST	11940	49749	87.98.245.48	192.168.2.3
May 11, 2021 20:02:27.916582108 CEST	49751	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:28.171042919 CEST	10090	49751	87.98.245.48	192.168.2.3
May 11, 2021 20:02:28.725832939 CEST	49751	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:29.084631920 CEST	10090	49751	87.98.245.48	192.168.2.3
May 11, 2021 20:02:29.616579056 CEST	49751	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:29.918757915 CEST	10090	49751	87.98.245.48	192.168.2.3
May 11, 2021 20:02:31.867494106 CEST	49752	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:32.117743015 CEST	11940	49752	87.98.245.48	192.168.2.3
May 11, 2021 20:02:32.726202011 CEST	49752	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:33.025172949 CEST	11940	49752	87.98.245.48	192.168.2.3
May 11, 2021 20:02:33.186909914 CEST	49753	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:33.480001926 CEST	10090	49753	87.98.245.48	192.168.2.3
May 11, 2021 20:02:33.616836071 CEST	49752	11940	192.168.2.3	87.98.245.48
May 11, 2021 20:02:33.847836018 CEST	11940	49752	87.98.245.48	192.168.2.3
May 11, 2021 20:02:34.040884018 CEST	49753	10090	192.168.2.3	87.98.245.48
May 11, 2021 20:02:34.270885944 CEST	10090	49753	87.98.245.48	192.168.2.3
May 11, 2021 20:02:34.929462910 CEST	49753	10090	192.168.2.3	87.98.245.48

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:01:07.004765034 CEST	51281	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:07.038886070 CEST	49199	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:07.066556931 CEST	53	51281	8.8.8.8	192.168.2.3
May 11, 2021 20:01:07.098418951 CEST	53	49199	8.8.8.8	192.168.2.3
May 11, 2021 20:01:07.494817972 CEST	50620	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:07.548559904 CEST	53	50620	8.8.8.8	192.168.2.3
May 11, 2021 20:01:09.228950977 CEST	64938	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:09.278584003 CEST	53	64938	8.8.8.8	192.168.2.3
May 11, 2021 20:01:10.152699947 CEST	60152	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:10.162095070 CEST	57544	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:10.202456951 CEST	53	60152	8.8.8.8	192.168.2.3
May 11, 2021 20:01:10.224232912 CEST	53	57544	8.8.8.8	192.168.2.3
May 11, 2021 20:01:11.907697916 CEST	55984	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:11.959342957 CEST	53	55984	8.8.8.8	192.168.2.3
May 11, 2021 20:01:13.059474945 CEST	64185	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:13.109622955 CEST	53	64185	8.8.8.8	192.168.2.3
May 11, 2021 20:01:15.595402002 CEST	65110	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:15.644582033 CEST	53	65110	8.8.8.8	192.168.2.3
May 11, 2021 20:01:16.662657022 CEST	58361	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:16.714410067 CEST	53	58361	8.8.8.8	192.168.2.3
May 11, 2021 20:01:17.499386072 CEST	63492	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:17.548319101 CEST	53	63492	8.8.8.8	192.168.2.3
May 11, 2021 20:01:18.377249956 CEST	60831	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:18.428778887 CEST	53	60831	8.8.8.8	192.168.2.3
May 11, 2021 20:01:19.277311087 CEST	60100	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:19.326052904 CEST	53	60100	8.8.8.8	192.168.2.3
May 11, 2021 20:01:20.349581957 CEST	53195	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:20.401139021 CEST	53	53195	8.8.8.8	192.168.2.3
May 11, 2021 20:01:21.546789885 CEST	50141	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:21.603723049 CEST	53	50141	8.8.8.8	192.168.2.3
May 11, 2021 20:01:22.402873993 CEST	53023	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:22.451591969 CEST	53	53023	8.8.8.8	192.168.2.3
May 11, 2021 20:01:23.730110884 CEST	49563	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:23.779150009 CEST	53	49563	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:01:24.779067993 CEST	51352	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:24.827877998 CEST	53	51352	8.8.8.8	192.168.2.3
May 11, 2021 20:01:34.007759094 CEST	59349	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:34.064801931 CEST	53	59349	8.8.8.8	192.168.2.3
May 11, 2021 20:01:35.142046928 CEST	57084	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:35.190892935 CEST	53	57084	8.8.8.8	192.168.2.3
May 11, 2021 20:01:37.435523033 CEST	58823	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:37.487049103 CEST	53	58823	8.8.8.8	192.168.2.3
May 11, 2021 20:01:38.464363098 CEST	57568	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:38.514513969 CEST	53	57568	8.8.8.8	192.168.2.3
May 11, 2021 20:01:41.509277105 CEST	50540	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:41.686825037 CEST	53	50540	8.8.8.8	192.168.2.3
May 11, 2021 20:01:45.616272926 CEST	54366	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:45.680080891 CEST	53	54366	8.8.8.8	192.168.2.3
May 11, 2021 20:01:49.138422966 CEST	53034	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:49.299673080 CEST	53	53034	8.8.8.8	192.168.2.3
May 11, 2021 20:01:53.265803099 CEST	57762	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:53.340054989 CEST	53	57762	8.8.8.8	192.168.2.3
May 11, 2021 20:01:54.340051889 CEST	55435	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:54.397157907 CEST	53	55435	8.8.8.8	192.168.2.3
May 11, 2021 20:01:55.685375929 CEST	50713	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:55.742697001 CEST	53	50713	8.8.8.8	192.168.2.3
May 11, 2021 20:01:58.142092943 CEST	56132	53	192.168.2.3	8.8.8.8
May 11, 2021 20:01:58.199521065 CEST	53	56132	8.8.8.8	192.168.2.3
May 11, 2021 20:02:01.318304062 CEST	58987	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:01.377551079 CEST	53	58987	8.8.8.8	192.168.2.3
May 11, 2021 20:02:02.242511034 CEST	56579	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:02.291301012 CEST	53	56579	8.8.8.8	192.168.2.3
May 11, 2021 20:02:03.740212917 CEST	60633	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:03.788909912 CEST	53	60633	8.8.8.8	192.168.2.3
May 11, 2021 20:02:08.667450905 CEST	61292	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:08.726759911 CEST	53	61292	8.8.8.8	192.168.2.3
May 11, 2021 20:02:12.782820940 CEST	63619	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:12.839679003 CEST	53	63619	8.8.8.8	192.168.2.3
May 11, 2021 20:02:16.987337112 CEST	64938	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:17.026994944 CEST	61946	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:17.047297001 CEST	53	64938	8.8.8.8	192.168.2.3
May 11, 2021 20:02:17.087491035 CEST	53	61946	8.8.8.8	192.168.2.3
May 11, 2021 20:02:18.992469072 CEST	64910	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:19.051923037 CEST	53	64910	8.8.8.8	192.168.2.3
May 11, 2021 20:02:24.215464115 CEST	52123	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:24.275331974 CEST	53	52123	8.8.8.8	192.168.2.3
May 11, 2021 20:02:25.024122953 CEST	56130	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:25.083309889 CEST	53	56130	8.8.8.8	192.168.2.3
May 11, 2021 20:02:26.134937048 CEST	56338	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:26.204402924 CEST	53	56338	8.8.8.8	192.168.2.3
May 11, 2021 20:02:27.854428053 CEST	59420	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:27.914695978 CEST	53	59420	8.8.8.8	192.168.2.3
May 11, 2021 20:02:31.807564974 CEST	58784	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:31.865056992 CEST	53	58784	8.8.8.8	192.168.2.3
May 11, 2021 20:02:33.124355078 CEST	63978	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:33.185776949 CEST	53	63978	8.8.8.8	192.168.2.3
May 11, 2021 20:02:39.061223030 CEST	62938	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:39.118395090 CEST	53	62938	8.8.8.8	192.168.2.3
May 11, 2021 20:02:45.022650957 CEST	55708	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:45.071504116 CEST	53	55708	8.8.8.8	192.168.2.3
May 11, 2021 20:02:54.950963974 CEST	56803	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:55.106497049 CEST	53	56803	8.8.8.8	192.168.2.3
May 11, 2021 20:02:55.939254045 CEST	57145	53	192.168.2.3	8.8.8.8
May 11, 2021 20:02:56.006665945 CEST	53	57145	8.8.8.8	192.168.2.3
May 11, 2021 20:03:00.298666954 CEST	55359	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:00.347470999 CEST	53	55359	8.8.8.8	192.168.2.3
May 11, 2021 20:03:00.979793072 CEST	58306	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:01.040043116 CEST	53	58306	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 20:03:06.509145021 CEST	64124	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:06.566308022 CEST	53	64124	8.8.8.8	192.168.2.3
May 11, 2021 20:03:06.962580919 CEST	49361	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:07.019815922 CEST	53	49361	8.8.8.8	192.168.2.3
May 11, 2021 20:03:08.108690977 CEST	63150	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:08.179083109 CEST	53	63150	8.8.8.8	192.168.2.3
May 11, 2021 20:03:10.875622034 CEST	53279	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:10.933634043 CEST	53	53279	8.8.8.8	192.168.2.3
May 11, 2021 20:03:16.381038904 CEST	56881	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:16.433048010 CEST	53	56881	8.8.8.8	192.168.2.3
May 11, 2021 20:03:21.888761044 CEST	53642	53	192.168.2.3	8.8.8.8
May 11, 2021 20:03:21.940306902 CEST	53	53642	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 20:01:41.509277105 CEST	192.168.2.3	8.8.8.8	0xdc43	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:01:49.138422966 CEST	192.168.2.3	8.8.8.8	0xfdd3	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:01:54.340051889 CEST	192.168.2.3	8.8.8.8	0x3f92	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:01:55.685375929 CEST	192.168.2.3	8.8.8.8	0x6470	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:01:58.142092943 CEST	192.168.2.3	8.8.8.8	0x8b06	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:08.667450905 CEST	192.168.2.3	8.8.8.8	0xc699	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:12.782820940 CEST	192.168.2.3	8.8.8.8	0xa310	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:17.026994944 CEST	192.168.2.3	8.8.8.8	0x9bb6	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:18.992469072 CEST	192.168.2.3	8.8.8.8	0x9788	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:24.215464115 CEST	192.168.2.3	8.8.8.8	0x6bf9	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:25.024122953 CEST	192.168.2.3	8.8.8.8	0x23e1	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:27.854428053 CEST	192.168.2.3	8.8.8.8	0xb19e	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:31.807564974 CEST	192.168.2.3	8.8.8.8	0xfb83	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:33.124355078 CEST	192.168.2.3	8.8.8.8	0x1f14	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:39.061223030 CEST	192.168.2.3	8.8.8.8	0xf4f9	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:45.022650957 CEST	192.168.2.3	8.8.8.8	0x6655	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:02:54.950963974 CEST	192.168.2.3	8.8.8.8	0x2f8a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:00.298666954 CEST	192.168.2.3	8.8.8.8	0xc300	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:00.979793072 CEST	192.168.2.3	8.8.8.8	0x8706	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:06.509145021 CEST	192.168.2.3	8.8.8.8	0x48a4	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:06.962580919 CEST	192.168.2.3	8.8.8.8	0xf1e5	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:10.875622034 CEST	192.168.2.3	8.8.8.8	0xff27	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:16.381038904 CEST	192.168.2.3	8.8.8.8	0x7101	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 11, 2021 20:03:21.888761044 CEST	192.168.2.3	8.8.8.8	0x307e	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

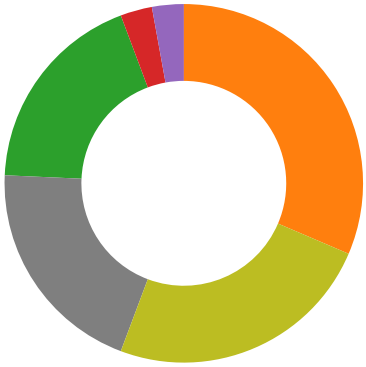
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 20:01:41.686825037 CEST	8.8.8.8	192.168.2.3	0xdc43	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 20:01:49.299673080 CEST	8.8.8.8	192.168.2.3	0xfdd3	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:01:54.397157907 CEST	8.8.8.8	192.168.2.3	0x3f92	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:01:55.742697001 CEST	8.8.8.8	192.168.2.3	0x6470	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:01:58.199521065 CEST	8.8.8.8	192.168.2.3	0x8b06	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:08.726759911 CEST	8.8.8.8	192.168.2.3	0xc699	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:12.839679003 CEST	8.8.8.8	192.168.2.3	0xa310	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:17.087491035 CEST	8.8.8.8	192.168.2.3	0x9bb6	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:19.051923037 CEST	8.8.8.8	192.168.2.3	0x9788	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:24.275331974 CEST	8.8.8.8	192.168.2.3	0x6bf9	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:25.083309889 CEST	8.8.8.8	192.168.2.3	0x23e1	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:27.914695978 CEST	8.8.8.8	192.168.2.3	0xb19e	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:31.865056992 CEST	8.8.8.8	192.168.2.3	0xfb83	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:33.185776949 CEST	8.8.8.8	192.168.2.3	0x1f14	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:39.118395090 CEST	8.8.8.8	192.168.2.3	0xf4f9	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:45.071504116 CEST	8.8.8.8	192.168.2.3	0x6655	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:02:55.106497049 CEST	8.8.8.8	192.168.2.3	0x2f8a	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:00.347470999 CEST	8.8.8.8	192.168.2.3	0xc300	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:01.040043116 CEST	8.8.8.8	192.168.2.3	0x8706	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:06.566308022 CEST	8.8.8.8	192.168.2.3	0x48a4	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:07.019815922 CEST	8.8.8.8	192.168.2.3	0xf1e5	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:10.933634043 CEST	8.8.8.8	192.168.2.3	0xff27	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:16.433048010 CEST	8.8.8.8	192.168.2.3	0x7101	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)
May 11, 2021 20:03:21.940306902 CEST	8.8.8.8	192.168.2.3	0x307e	No error (0)	sys2021.linkpc.net		87.98.245.48	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6380 Parent PID: 3388

General

Start time:	20:01:15
Start date:	11/05/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice No F1019855_PDF.vbs'
Imagebase:	0x7ff78dde0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: file.exe PID: 6588 Parent PID: 6380

General

Start time:	20:01:20
Start date:	11/05/2021
Path:	C:\Users\user\AppData\Local\Temp\file.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\file.exe'
Imagebase:	0xd70000
File size:	703488 bytes
MD5 hash:	E6A6EB2982AB17BBB7083493805823BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000003.00000002.255078777.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.256966112.00000000040F9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC0CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC0CF06	unknown
C:\Users\user\AppData\Roaming\JkeJLChUI.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA51E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpAD9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA57038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF1C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAD9.tmp	success or wait	1	6CA56A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JkeJLChUI.exe	unknown	703488	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 32 47 5a b7 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b2 0a 00 00 08 00 00 00 00 00 00 56 d1 0a 00 00 20 00 00 00 e0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 20 0b 00 00 02 00 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...2GZ..... ....0.....V.... .....@.. ....@.....	success or wait	1	6CA51B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpAD9.tmp	unknown	1642	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CA51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	unknown	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DF1C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA51B4F	ReadFile
unknown	unknown	703488	success or wait	1	6CA51B4F	ReadFile

Analysis Process: name.exe PID: 6612 Parent PID: 6380

General

Start time:	20:01:20
Start date:	11/05/2021
Path:	C:\Users\user\AppData\Local\Temp\name.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\name.exe'
Imagebase:	0xcd0000
File size:	784896 bytes
MD5 hash:	43C4F163196FF02E7AA8C5040375FDA4

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: 00000004.00000002.254692678.0000000004551000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.254692678.0000000004551000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.254692678.0000000004551000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	730560AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	730560AC	unknown
C:\Users\user\AppData\Roaming\LiydYED.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	59016AB	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC12.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	16DB788	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\name.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	730434A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC12.tmp	success or wait	1	5902322	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LiydYED.exe	unknown	784896	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e9 c9 63 e9 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 f0 0b 00 00 08 00 00 00 00 00 00 3a 0e 0c 00 00 20 00 00 00 20 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....c........... ....0.............:.... ... .@.. ....` ....@................	success or wait	1	5901933	WriteFile
C:\Users\user\AppData\Local\Temp\tmpC12.tmp	unknown	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	5901933	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\name.exe.log	unknown	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	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,"	success or wait	1	7332A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73085544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73085544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73088738	ReadFile
C:\Users\user\AppData\Local\Temp\name.exe	unknown	784896	success or wait	1	5901933	ReadFile

Analysis Process: schtasks.exe PID: 7072 Parent PID: 6588

General

Start time:	20:01:36
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JkeJLChUI' /XML 'C:\Users\user\AppData\Local\Temp\tmpAD9.tmp'
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAD9.tmp	unknown	2	success or wait	1	2AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAD9.tmp	unknown	1643	success or wait	1	2AABD9	ReadFile

Analysis Process: schtasks.exe PID: 7088 Parent PID: 6612

General

Start time:	20:01:36
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LiydYED' /XML 'C:\Users\user\AppData\Local\Temp\tmpC12.tmp'
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC12.tmp	unknown	2	success or wait	1	2AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC12.tmp	unknown	1641	success or wait	1	2AABD9	ReadFile

Analysis Process: conhost.exe PID: 7104 Parent PID: 7072

General

Start time:	20:01:37
Start date:	11/05/2021
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: conhost.exe PID: 7116 Parent PID: 7088

General

Start time:	20:01:37
Start date:	11/05/2021
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: file.exe PID: 7156 Parent PID: 6588

General

Start time:	20:01:37
Start date:	11/05/2021
Path:	C:\Users\user\AppData\Local\Temp\file.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd60000
File size:	703488 bytes
MD5 hash:	E6A6EB2982AB17BBB7083493805823BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000A.00000002.468822970.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC0CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC0CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA51B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: name.exe PID: 800 Parent PID: 6612

General

Start time:	20:01:38
Start date:	11/05/2021
Path:	C:\Users\user\AppData\Local\Temp\name.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x980000
File size:	784896 bytes
MD5 hash:	43C4F163196FF02E7AA8C5040375FDA4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.477861276.0000000005590000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.477861276.0000000005590000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.476715022.0000000004087000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.476715022.0000000004087000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.468941603.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.468941603.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.468941603.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.478086503.0000000005950000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.478086503.0000000005950000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.478086503.0000000005950000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	730560AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	730560AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53407A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	534089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53407A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53407A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	730560AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	730560AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	f6 33 d7 43 f2 14 d9 48	.3.C...H	success or wait	1	5340A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73085544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73085544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73088738	ReadFile
C:\Users\user\AppData\Local\Temp\name.exe	unknown	4096	success or wait	1	7312BF06	unknown
C:\Users\user\AppData\Local\Temp\name.exe	unknown	512	success or wait	1	7312BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73085544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73085544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5340A53	ReadFile

Disassembly

Code Analysis