ID: 402352
Sample Name: DHLAWB# 9284880911 pdf.exe
Cookbook: default.jbs
Time: 04:09:21
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

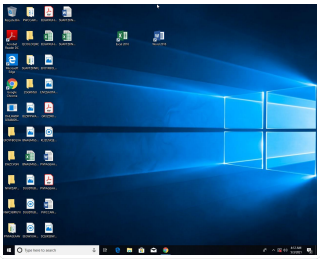
Analysis Report DHLAWB# 9284880911 pdf.exe

Overview

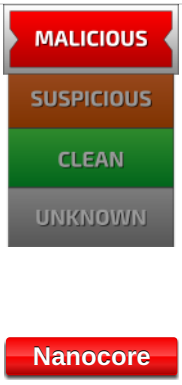
General Information

Sample Name:	DHLAWB# 9284880911 pdf.exe
Analysis ID:	402352
MD5:	72208e35ab96b5..
SHA1:	ca1a5cefafcd9e4...
SHA256:	a2bb219a5ecfa04.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



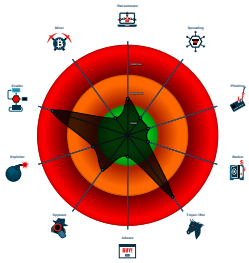
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- DHLAWB# 9284880911 pdf.exe (PID: 3012 cmdline: 'C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe' MD5: 72208E35AB96B53BAFFD99165D2F50CB)
  - schtasks.exe (PID: 3468 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HVLIxSqWJDWWZt' /XML 'C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHLAWB# 9284880911 pdf.exe (PID: 1560 cmdline: C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe MD5: 72208E35AB96B53BAFFD99165D2F50CB)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "97a824b7-e666-4a22-b2e3-fb501d91",
  "Group": "king",
  "Domain1": "23.105.131.171",
  "Domain2": "",
  "Port": 4040,
  "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"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.483729377.0000000005B80000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000004.00000002.483729377.0000000005B80000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000004.00000002.472666786.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.472666786.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.472666786.0000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.DHLAWB# 9284880911 pdf.exe.38647fc.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
4.2.DHLAWB# 9284880911 pdf.exe.38647fc.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated

Source	Rule	Description	Author	Strings
0.2.DHLAWB# 9284880911 pdf.exe.46f7978.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x429ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x429ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.DHLAWB# 9284880911 pdf.exe.46f7978.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x42725:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x429ad:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x43fe6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x43fda:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x44e8b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x4ac42:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost • 0x429d7:$s5: IClientLoggingHost
0.2.DHLAWB# 9284880911 pdf.exe.46f7978.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 54 entries				

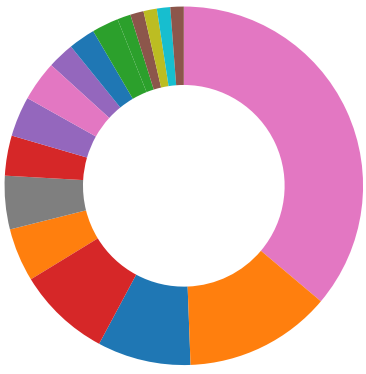
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

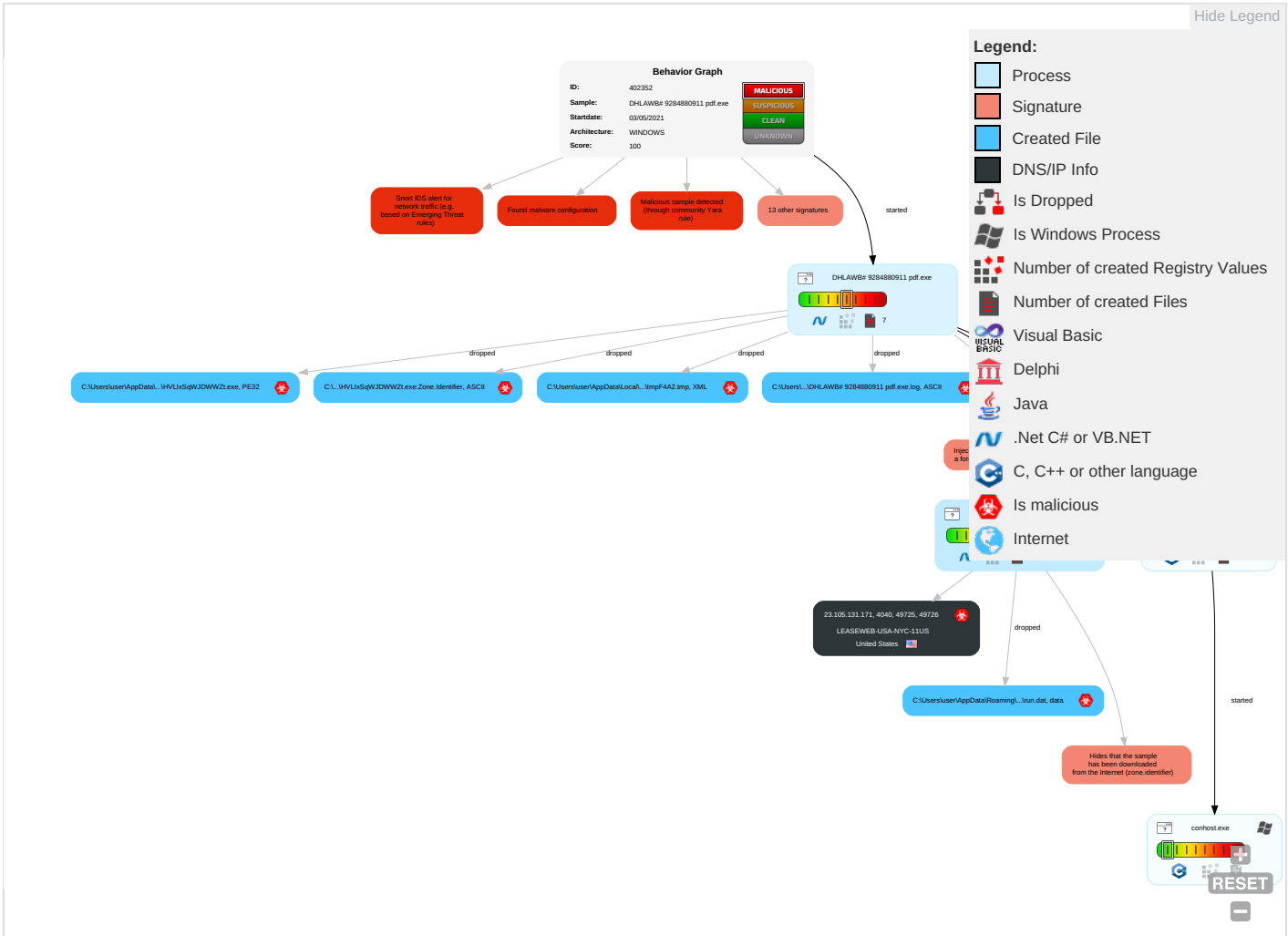
Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHLAWB# 9284880911 pdf.exe	11%	ReversingLabs		
DHLAWB# 9284880911 pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe	11%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.DHLAWB# 9284880911 pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.DHLAWB# 9284880911 pdf.exe.60b0000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krtriFH	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.jiyu-kobo.co.jp/a-e	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comceTF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/TS	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.sandoll.co.krZ	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnb-n	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.founder.com.cn/cnerslH	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/MI:H	0%	Avira URL Cloud	safe	
http://www.fonts.com-uA	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kre	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.tiro.comtn	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ko	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ito	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
23.105.131.171	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.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/jp/8T	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comibiT	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cns-m	0%	Avira URL Cloud	safe	
http://www.tiro.comh	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnk-s	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/RT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/liquwT	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
23.105.131.171	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

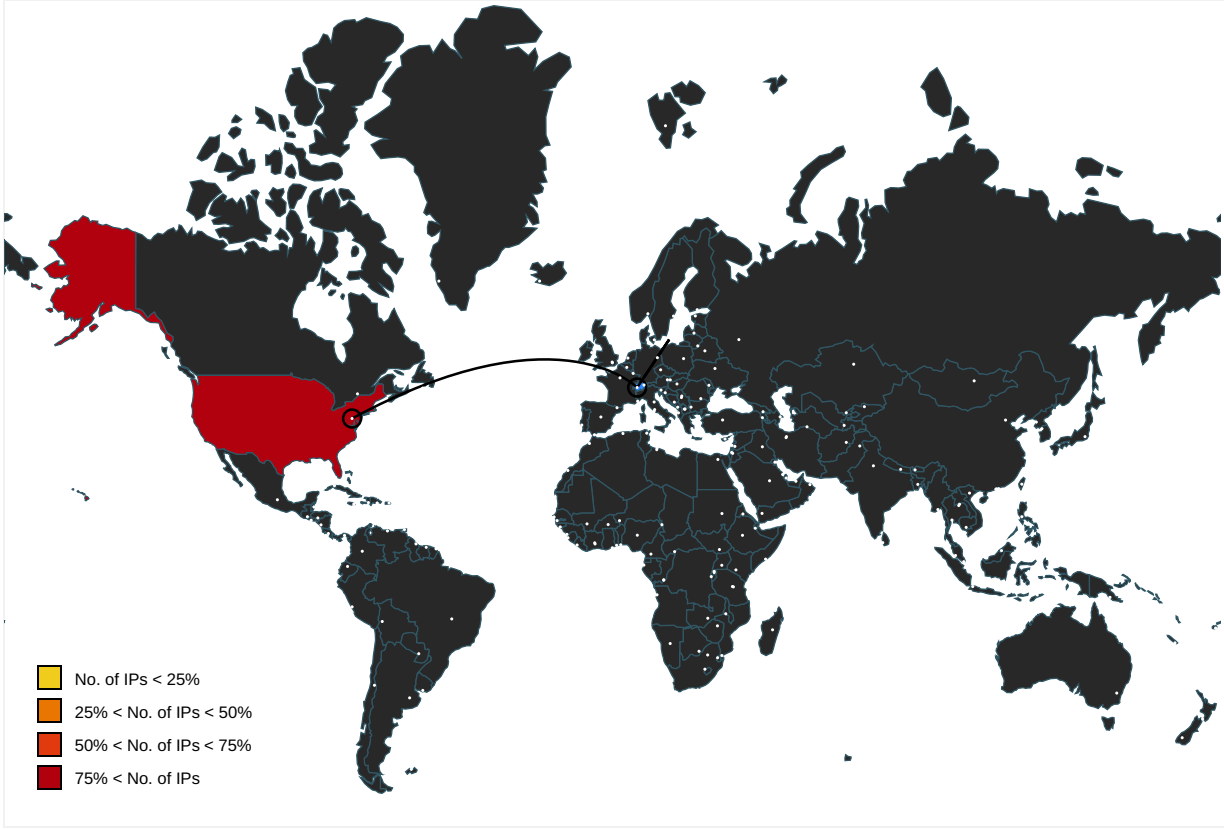
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krtriFH	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208289981.000000005886000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a-e	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false		high
http://www.tiro.com	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp, DHLAWB# 9284880911 pdf.exe, 00000000.00000003.212524209.000000000588D000.00000004.00000001.sdmp, DHLAWB# 9284880911 pdf.exe, 00000000.00000003.212025172.0000000005889000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comceTF	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.226163799.000000005880000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/TS	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208864496.000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.227902373.000000003540000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207260612.00000000589B000.00000004.00000001.sdmp, DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krZ	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208289981.000000005886000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207425359.00000000589B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnb-n	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208693548.00000000058BD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.00000000005884000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnerslH	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208864496.00000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.00000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.00000000005884000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207382725.00000000000589B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.00000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.00000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.00000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.00000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.00000000006B12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.226163799.00000000005880000.00000004.00000001.sdmp	false		high
http://www.fonts.comc	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207382725.00000000000589B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/MI:H	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208706639.00000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com-uA	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207382725.00000000000589B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kre	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208289981.00000000005886000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.00000000005884000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comtn	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207580705.00000000000589B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207004883.00000000000195D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ko	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.00000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ito	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.0000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208864496.0000000005884000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208864496.0000000005884000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.0000000005884000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/8T	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.0000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	DHLAWB# 9284880911 pdf.exe, 00000000.00000002.232662327.0000000006B12000.00000004.00000001.sdmp, DHLAWB# 9284880911 pdf.exe, 00000000.00000003.212524209.000000000588D000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comibiT	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207260612.0000000000589B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cns-m	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208693548.00000000058BD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comh	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.207630084.0000000000589B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnk-s	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.208693548.00000000058BD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/RT	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.0000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/liquwT	DHLAWB# 9284880911 pdf.exe, 00000000.00000003.209977218.0000000005884000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.105.131.171	unknown	United States		396362	LEASEWEB-USA-NYC-11US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402352
Start date:	03.05.2021
Start time:	04:09:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHLAWB# 9284880911 pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/6@0/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:10:17	API Interceptor	991x Sleep call for process: DHLAWB# 9284880911 pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	PO.pdf.exe	Get hash	malicious	Browse	• 23.105.131.190
	PO.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	SecuriteInfo.com.Trojan.Win32.Save.a.29244.exe	Get hash	malicious	Browse	• 23.105.131.161
	ZBgnuLqtOd.exe	Get hash	malicious	Browse	• 23.105.131.161
	ZE9u48l6N4.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO copy.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	invoice&packing list.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO.PDF.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO copy.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	Ordem urgente AWB674653783- FF2453,PDF.exe	Get hash	malicious	Browse	• 23.105.131.132
	Remittance FormDoc.exe	Get hash	malicious	Browse	• 23.19.227.243
	Presupuesto de orden urgente KTX88467638,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	Dringende Bestellung Zitat CTX88467638,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	shipping document.exe	Get hash	malicious	Browse	• 23.105.131.207
	6V9espP5wD.exe	Get hash	malicious	Browse	• 23.105.131.195
	NVAbIqNO9h.exe	Get hash	malicious	Browse	• 23.105.131.209
	UUGCfhIdFD.exe	Get hash	malicious	Browse	• 23.105.131.228
	KPcrOQcb5P.exe	Get hash	malicious	Browse	• 23.105.131.228
	rGsJ1mXomJ.exe	Get hash	malicious	Browse	• 23.105.131.228

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DHLAWB# 9284880911 pdf.exe.log	
Process:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp	
Process:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.207288139039549
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBhjtn:cbh47TlNQ//rydbz9I3YODOLNdq3rx
MD5:	68BA3B143C5974B5DED04F92F7827666
SHA1:	F8BE95A25B6028A32CB00EC509277E43C8F6B745
SHA-256:	B12C7C79B35BF6F2B71A1D379C60D69F3B29F63D887CAF320FAFE74FC029A612
SHA-512:	667D269D27739268F1B37BF193CE05EF88CFE5B60561AFFE0E2C44F988C7C4EA1C300707B2A7616CC0793095F04AD1022EF8A04369F4144D0A54B181BBC72430
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwh:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	0FBED11864C03FDED0E70014DCF84578
SHA1:	453723D938A03252F705B0A104986FE4C5CA7056
SHA-256:	70F5E49EE3091777827ED661B63842061220C899A708860986E9AA1BD87C5004
SHA-512:	DB53E3F1D18171F1D86C1B9BBF6BBD07153FC3E561834A35834BC0CA1E034FEDCD83AAAE7EDF9262C4E175C3D2287B647F55282E49627EAAF587F4371420466
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:26Vt:26H
MD5:	62A6C13CD893BCE61252A1FBDEF3D1E7
SHA1:	D600274F5EC2D00AFA5248B17FC1AF3D26B618E6
SHA-256:	3AB5689F7F661B5857C8B9B89ED75FBE1E672C1D1FB6503EBC7F7C27D37DC5A3
SHA-512:	8DEE624F1D97EF4B30336D5534389659A251F26D0E6CEC1ECA7B8AE283AFA014EF3D86BD7121172D97D54A26838A47BE86843220EE4FF2631766E25650888EE8
Malicious:	**true**
Reputation:	low
Preview:	.f_.$..H

C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe	
Process:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	791040
Entropy (8bit):	7.913655996564074
Encrypted:	false
SSDEEP:	12288:25+tz1qUQFb6Jn7Hqty7Q6gUKljtD8hgeo2JvKy12cmLqfnkp6gM:2oJ1qLFba7QyE6ghVt8geJ52cmLqf5g
MD5:	72208E35AB96B53BAFFD99165D2F50CB
SHA1:	CA1A5CEFAFCD9E4F37BB3880D96AA0FB86043CF1
SHA-256:	A2BB219A5ECFA042DC97A47AEDA8A637F49E70E09AF3F7B52F7974F7B1C39172
SHA-512:	71D28A8965CDDF7968804AC0FC446C8A303FE860555818C98F98962810EB459D0422B6EEAF86A40620EDE4226901EAFB0330E12C1188ADB3884412EB03F02E28
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...NM.`.....P.....$... ...@....@.. ..... ..@.....$..O....@..4.....`.....P#..... ....H.....text..... ....`.rsrc...4....@.....@..@.rel oc.....`.....@..B.....$.....H.....4.....8>.....0.....(....(.....(.....o.....*.....(.....(.....(!.....("....(#....*N..(....oe... ($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,!r...p.....(1...o2...s3.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.913655996564074
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DHLAWB# 9284880911 pdf.exe
File size:	791040
MD5:	72208e35ab96b53baffd99165d2f50cb
SHA1:	ca1a5cefafcd9e4f37bb3880d96aa0fb86043cf1
SHA256:	a2bb219a5ecfa042dc97a47aeda8a637f49e70e09af3f7b52f7974f7b1c39172
SHA512:	71d28a8965cddf7968804ac0fc446c8a303fe860555818c98f98962810eb459d0422b6eeaf86a40620ede4226901efb0330e12c1188adb3884412eb03f02e28
SSDEEP:	12288:25+tz1qUQFb6Jn7Hqty7Q6gUKljtD8hgeo2JvKy12cmLqfnkp6gM:2oJ1qLFba7QyE6ghVt8geJ52cmLqf5g
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...NM.`.....P.....$.. ...@....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c24da
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608F4D4E [Mon May 3 01:09:34 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2488	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x634	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc2350	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc04e0	0xc0600	False	0.935686474578	data	7.92145067275	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x634	0x800	False	0.33984375	data	3.51853256281	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc4090	0x3a4	data		
RT_MANIFEST	0xc4444	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Opti-Tek
Assembly Version	1.0.1.7
InternalName	StringHandleOnStack.exe
FileVersion	1.0.1.7
CompanyName	Opti-Tek
LegalTrademarks	
Comments	Machine Operator
ProductName	InternalArrayTypeE
ProductVersion	1.0.1.7
FileDescription	InternalArrayTypeE
OriginalFilename	StringHandleOnStack.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-04:10:23.692897	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	4040	192.168.2.3	23.105.131.171
05/03/21-04:10:29.991238	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	4040	192.168.2.3	23.105.131.171
05/03/21-04:10:36.191569	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	4040	192.168.2.3	23.105.131.171
05/03/21-04:10:42.540681	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	4040	192.168.2.3	23.105.131.171
05/03/21-04:10:47.683486	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	4040	192.168.2.3	23.105.131.171
05/03/21-04:10:53.831453	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:00.147141	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:06.368003	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:12.549875	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:18.828670	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:25.226719	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:32.050089	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:38.190410	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:44.381807	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:50.630024	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	4040	192.168.2.3	23.105.131.171
05/03/21-04:11:56.886506	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	4040	192.168.2.3	23.105.131.171
05/03/21-04:12:02.999852	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	4040	192.168.2.3	23.105.131.171
05/03/21-04:12:09.279030	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	4040	192.168.2.3	23.105.131.171
05/03/21-04:12:15.429008	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	4040	192.168.2.3	23.105.131.171

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 04:10:23.308895111 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:23.637084007 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:23.637183905 CEST	49725	4040	192.168.2.3	23.105.131.171

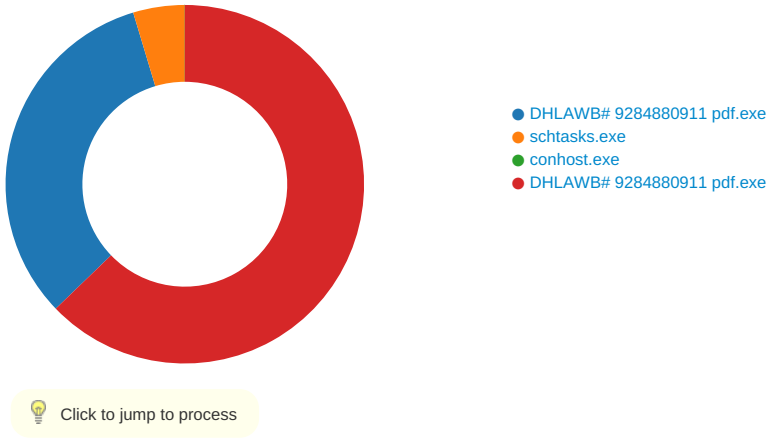
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 04:10:23.692897081 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:24.038207054 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:24.038295031 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:24.431047916 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:24.431204081 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:24.761238098 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:24.761467934 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.142074108 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.142237902 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.524909973 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.525513887 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.538619041 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.538675070 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.538707018 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.538757086 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.539366007 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.539419889 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.540429115 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.540513039 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.540590048 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.541428089 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.541517973 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.541542053 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.541850090 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.542438030 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.542567015 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.542603970 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.542740107 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.543353081 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.543406963 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.577517986 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.869527102 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.869627953 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.870480061 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.870650053 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.870682955 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.870731115 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.871331930 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.871392012 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.871515036 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.871557951 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.872340918 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.872395039 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.872596025 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.873377085 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.873459101 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.873682976 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.874253035 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.874397993 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.874519110 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.874548912 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.874629974 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.875372887 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.875430107 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.875561953 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.875614882 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.876296043 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.876339912 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.877504110 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.877588034 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.877597094 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.879426956 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.879489899 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.880337000 CEST	4040	49725	23.105.131.171	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 04:10:25.880518913 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.880577087 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:25.881630898 CEST	4040	49725	23.105.131.171	192.168.2.3
May 3, 2021 04:10:25.881704092 CEST	49725	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:29.655863047 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:29.987122059 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:29.988065004 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:29.991238117 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:30.338108063 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:30.338293076 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:30.708023071 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:30.708209038 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.043282986 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.043447018 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.413105965 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.413206100 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.791016102 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.791140079 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.826256037 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.826469898 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.826493025 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.826510906 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.826565027 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.826618910 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.826832056 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.827486992 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.827555895 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.827646971 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.827800035 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.828376055 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.828445911 CEST	49726	4040	192.168.2.3	23.105.131.171
May 3, 2021 04:10:31.828535080 CEST	4040	49726	23.105.131.171	192.168.2.3
May 3, 2021 04:10:31.828588009 CEST	49726	4040	192.168.2.3	23.105.131.171

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHLAWB# 9284880911 pdf.exe PID: 3012 Parent PID: 5620

General

Start time:	04:10:11
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe'
Imagebase:	0xe30000
File size:	791040 bytes
MD5 hash:	72208E35AB96B53BAFFD99165D2F50CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.230786532.0000000004501000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.230786532.0000000004501000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.230786532.0000000004501000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.227902373.0000000003540000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5500500	CopyFileW
C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5500500	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2F7B2F8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DHLAWB# 9284880911 pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp	success or wait	1	550126E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe	0	262144	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 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 4e 4d 8f 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 06 0c 00 00 0a 00 00 00 00 00 00 da 24 0c 00 00 20 00 00 00 40 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 80 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.... $.......PE..L...NM.`.......... ....P.............$... ...@....@.. ....@................	success or wait	4	5500500	CopyFileW
C:\Users\user\AppData\Roaming\HVLIxSqWJDWWZt.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	5500500	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp	unknown	1647	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/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	5500F2B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DHLAWB# 9284880911 pdf.exe.log	unknown	664	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 3468 Parent PID: 3012

General

Start time:	04:10:20
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HVLIxSqWJDWWZt' /XML 'C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp'
Imagebase:	0x190000
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\tmpF4A2.tmp	unknown	2	success or wait	1	19AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF4A2.tmp	unknown	1648	success or wait	1	19ABD9	ReadFile

Analysis Process: conhost.exe PID: 2168 Parent PID: 3468

General

Start time:	04:10:20
Start date:	03/05/2021
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: DHLAWB# 9284880911 pdf.exe PID: 1560 Parent PID: 3012

General

Start time:	04:10:21
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe
Imagebase:	0xfb0000
File size:	791040 bytes
MD5 hash:	72208E35AB96B53BAFFD99165D2F50CB
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: 00000004.00000002.483729377.0000000005B80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.483729377.0000000005B80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.472666786.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.472666786.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.472666786.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.481253287.000000000383B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.484302259.00000000060B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.484302259.00000000060B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.484302259.00000000060B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.482228223.00000000047E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.482228223.00000000047E1000.00000004.00000001.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	72FB60AC	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	72FB60AC	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	5AA07A1	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	5AA089B	CreateFileW
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	72FB60AC	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	72FB60AC	unknown
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	5AA07A1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	5AA07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5AA089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe:Zone.Identifier	success or wait	1	5AA0D41	DeleteFileA

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	15 66 5f 0b 24 0e d9 48	.f_.$..H	success or wait	1	5AA0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	5AA0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	9	5AA0A53	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5AA0A53	ReadFile
C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\DHLAWB# 9284880911 pdf.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5AA0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5AA0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown

Disassembly

Code Analysis