ID: 356502
Sample Name: Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
Cookbook: default.jbs
Time: 09:03:50
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

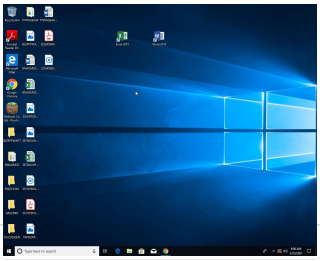
Analysis Report Skilmark Co. Ltd - Purchase Order 0220…

Overview

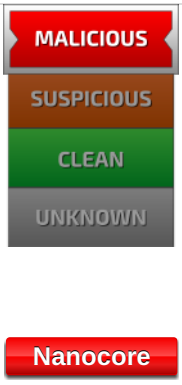
General Information

Sample Name:	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
Analysis ID:	356502
MD5:	d765dcbdabed2e..
SHA1:	be68fc678cca643..
SHA256:	d2693c3162e3ea..
Tags:	exe NanoCore

Most interesting Screenshot:



Detection



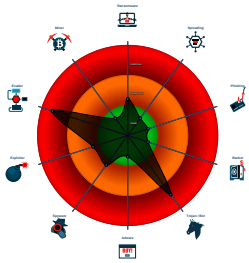
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- Skilmark Co. Ltd - Purchase Order 022021.pdf.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe' MD5: D765DCBDABED2ED1DD0FDD8800F221ED)
  - schtasks.exe (PID: 7004 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OEpDLNVZW' /XML 'C:\Users\user\AppData\Local\Temp\tmp8B36.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Skilmark Co. Ltd - Purchase Order 022021.pdf.exe (PID: 7048 cmdline: C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe MD5: D765DCBDABED2ED1DD0FDD8800F221ED)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.254941968.000000000411 3000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40f8d:$x1: NanoCore.ClientPluginHost • 0x737ad:$x1: NanoCore.ClientPluginHost • 0x40fca:$x2: IClientNetworkHost • 0x737ea:$x2: IClientNetworkHost • 0x44afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7731d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.254941968.000000000411 3000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.254941968.000000000411 3000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x40cf5:$a: NanoCore • 0x40d05:$a: NanoCore • 0x40f39:$a: NanoCore • 0x40f4d:$a: NanoCore • 0x40f8d:$a: NanoCore • 0x73515:$a: NanoCore • 0x73525:$a: NanoCore • 0x73759:$a: NanoCore • 0x7376d:$a: NanoCore • 0x737ad:$a: NanoCore • 0x40d54:$b: ClientPlugin • 0x40f56:$b: ClientPlugin • 0x40f96:$b: ClientPlugin • 0x73574:$b: ClientPlugin • 0x73776:$b: ClientPlugin • 0x737b6:$b: ClientPlugin • 0x40e7b:$c: ProjectData • 0x7369b:$c: ProjectData • 0x41882:$d: DESCrypto • 0x740a2:$d: DESCrypto • 0x4924e:$e: KeepAlive
00000000.00000002.253631018.0000000002EE 2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.253583069.0000000002E9 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.2ec6bf0.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.4143e00.4.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:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.4143e00.4.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.Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.4143e00.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.4143e00.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x42715:$a: NanoCore • 0x42725:$a: NanoCore • 0x42959:$a: NanoCore • 0x4296d:$a: NanoCore • 0x429ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x42774:$b: ClientPlugin • 0x42976:$b: ClientPlugin • 0x429b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x4289b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x432a2:$d: DESCrypto • 0x1844e:$e: KeepAlive
Click to see the 4 entries				

Sigma Overview

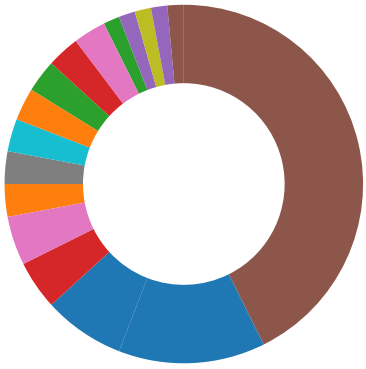
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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:

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

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains 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 AntiVM_3

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:

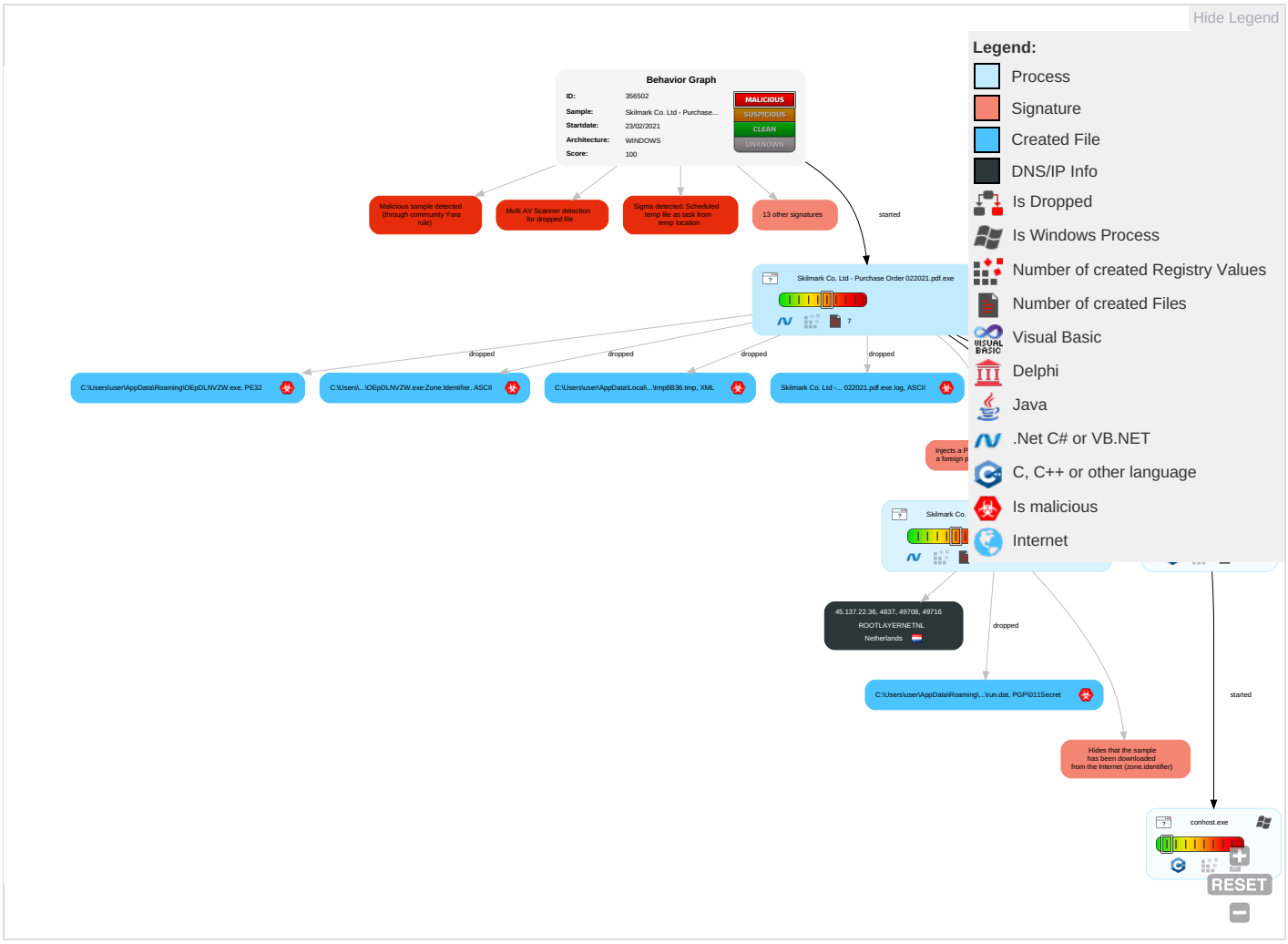
Detected Nanocore Rat

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	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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
Skilmark Co. Ltd - Purchase Order 022021.pdf.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	
Skilmark Co. Ltd - Purchase Order 022021.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\OEpDLNVZW.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\OEpDLNVZW.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmC	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/J	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/watg	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comoituJ	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.founder.com.cn/cnn	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0ld&	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.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.fontbureau.comF0	0%	Avira URL Cloud	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.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fonts.comic-	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/T	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/tendJ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceva	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/I	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtq	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/C	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/oi	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.jiyu-kobo.co.jp/?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/x	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.ascendercorp.com/typedesigners.htmlu	0%	Avira URL Cloud	safe	
http://www.urwpp.dev	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/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTFJ	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	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/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/g	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmC	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.222531315.0000000005EDA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

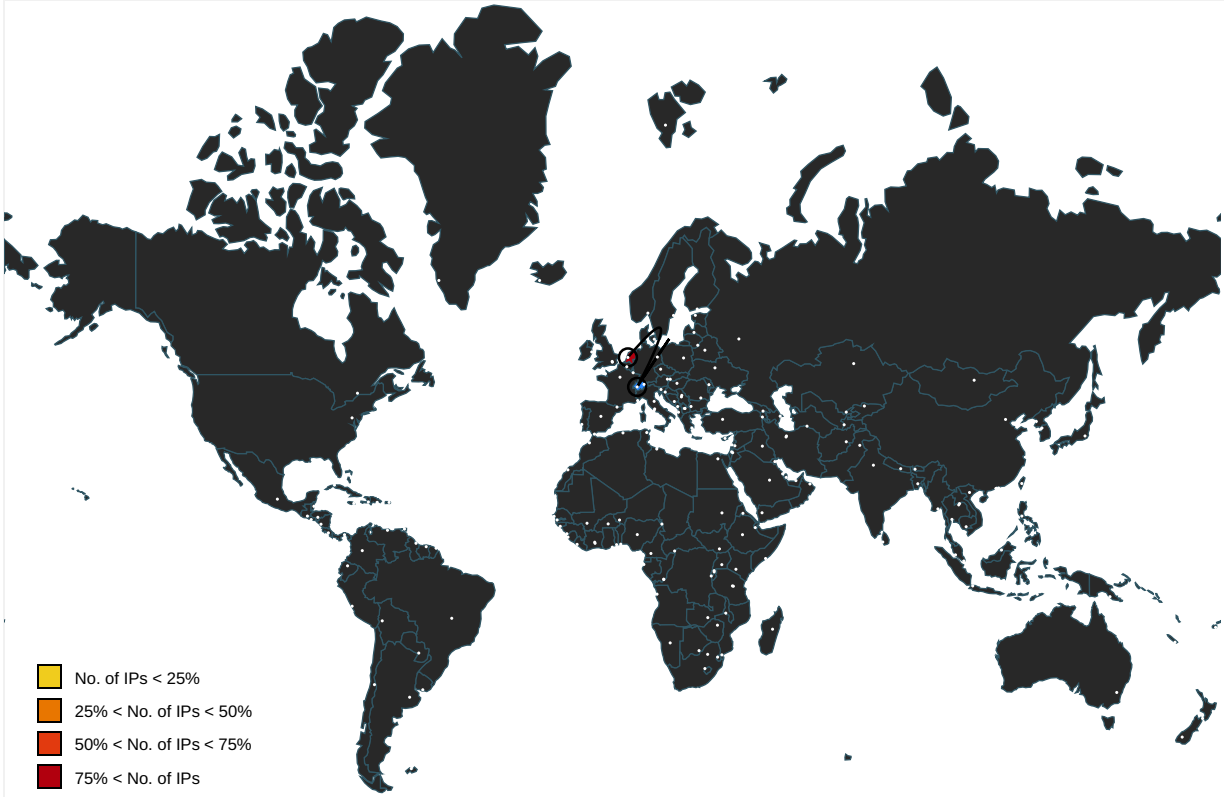
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/J	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/watg	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.218577225.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoituJ	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.223872505.0000000005EC3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.253631018.0000000002EE2000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp, Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.214009189.0000000005EC3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnn	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.215838737.0000000005ECE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/0	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219943805.0000000005F05000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0ld&	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221493033.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.253583069.0000000002E91000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comF0	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.224206853.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comalsd	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221493033.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com?	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221721195.0000000005EC7000.00000004.00000001.sdmp	false		high
http://www.fonts.comic-	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.214576676.0000000005EDB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.222198300.0000000005ED3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlh	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.220995450.0000000005ED9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comF	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221721195.0000000005EC7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/T	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/tendJ	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.218577225.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comceva	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.224206853.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/l	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.216253909.0000000005EC6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comtq	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.223872505.0000000005EC3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnz	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.215993988.0000000005EC7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/C	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/oi	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/?	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.220053478.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/x	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.htmlu	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219952811.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.dev	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221493033.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comI.TTFJ	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221721195.0000000005EC7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.223450253.0000000005ECC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp, Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000002.259016529.00000000070D2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/g	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.219183506.0000000005EC5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comM.TTF	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.221721195.0000000005EC7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/4	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.21 6202308.0000000005EC8000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.22 0665177.0000000005EFE000.00000 004.00000001.sdmp	false		high
http://www.tiro.comc$	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe, 00000000.00000003.21 4832365.0000000005EDB000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.22.36	unknown	Netherlands		51447	ROOTLAYERNETNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356502
Start date:	23.02.2021
Start time:	09:03:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Skilmark Co. Ltd - Purchase Order 022021.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@6/8@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 86% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356502/sample/Skilmark Co. Ltd - Purchase Order 022021.pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
09:04:50	API Interceptor	915x Sleep call for process: Skilmark Co. Ltd - Purchase Order 022021.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.137.22.36	Jagtap Trading - order #JEW-39-16.02.2021.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	SKM_C3350191107102300.exe	Get hash	malicious	Browse	• 185.222.58.152
	Jagtap Trading - order #JEW-39-16.02.2021.exe	Get hash	malicious	Browse	• 45.137.22.36
	AKBANK E-DEKONT.exe	Get hash	malicious	Browse	• 45.137.22.52
	New Order.exe	Get hash	malicious	Browse	• 45.137.22.102
	New Order.exe	Get hash	malicious	Browse	• 45.137.22.102
	LnkxrWO6yvd9qaJ.exe	Get hash	malicious	Browse	• 185.222.58.156
	tuesdacrypted.exe	Get hash	malicious	Browse	• 185.222.57.68
	000009000000900.exe	Get hash	malicious	Browse	• 45.137.22.52
	TT.exe	Get hash	malicious	Browse	• 185.222.57.213
	Cotizaci#U00f3n de factura.exe	Get hash	malicious	Browse	• 45.137.22.52
	kart-009000000..pdf...exe	Get hash	malicious	Browse	• 45.137.22.52
	PO-OIOI09000.exe	Get hash	malicious	Browse	• 45.137.22.52
	090000090000-090.exe	Get hash	malicious	Browse	• 45.137.22.52
	kart gecmisi.exe	Get hash	malicious	Browse	• 45.137.22.52
	000000000900R.exe	Get hash	malicious	Browse	• 45.137.22.52
	0000000000009000.exe	Get hash	malicious	Browse	• 45.137.22.52
	090887000008000000.exe	Get hash	malicious	Browse	• 45.137.22.52
	PURCHASE ORDER098090.exe	Get hash	malicious	Browse	• 45.137.22.52
	rawwwwwwwcrypted.exe	Get hash	malicious	Browse	• 185.222.57.68
	REMOUOOO9O9.exe	Get hash	malicious	Browse	• 45.137.22.52

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.log

Process:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, 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=b77a

C:\Users\user\AppData\Local\Temp\tmp8B36.tmp

Process:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.196417458630448
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBCtn:cbh47TlNQ//rydbz9l3YODOLNdq3+
MD5:	D9D1C867D06A3C4424E37DE3E7433EAE

C:\Users\user\AppData\Local\Temp\tmp8B36.tmp	
SHA1:	91B9B926B8EB63ABA169829EC238D0A95F9C3127
SHA-256:	94A1ECAAC917C26B04D29202121DEDDFCEB81DA3D6F667B81CF4F33A4E2F1017
SHA-512:	7B7CE1293379259E0DC8E46D60EC5BA90EE2AAE126223832AF4592142B1D632ED6CEAE0530A577070CA63945BA6831290442C7B45550724642B962ADC5C6BDE
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\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6B5
Malicious:	false
Reputation:	low
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\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:9a5ft:OF
MD5:	94B9CF650DCB8C2D129D5E8B1D940170
SHA1:	5C0A796FEBE9520A98018D1F36731E35DBAFCE62
SHA-256:	84F05EE5CD6B34BDB8092DFFC6DF97DFD0159089282BE74E80AF8CED0CE86125
SHA-512:	9301AE7A595C4C482E3446908B5A4DD1E1E8D3F7D287014A553082D07C211BF27F3B0359B94C6F3EBF9B7E2EAFD26606E966EC8D4FC34407FF1A4E22891A69E
Malicious:	**true**
Reputation:	low
Preview:	.-?)...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[.../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\OEpDLNVZW.exe	
Process:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	729088
Entropy (8bit):	7.373755208458107
Encrypted:	false
SSDEEP:	12288:xClJbGEIGv5dKbr/Yy1V5LYRs5dCJ/ninKUGTSZ+gFQ6CYjcMfNsKcRJN8P:OJ7IogPHZY8KfTScKNjcMfXcOP
MD5:	D765DCBDABED2ED1DD0FDD8800F221ED
SHA1:	BE68FC678CCA6434577D7AF59ABF129569AB7B47
SHA-256:	D2693C3162E3EA906BF7FC546A07985A3BF55BBFB78F52015265CF7140EED31F
SHA-512:	F4345F41A035C8D4502411A36001C4EE5A02D9F85F3FE00FC5DC97A7860470D545F9C0C1C1EEC1633ADCC391C1A326D6B4D3833E60C66A2DE50CD7D170D335
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....$.....PE..L...PH4`.....P.....".. ...@....@.. .....@.....!..O....@..D.....`..... ....H.....text..... ....`.rsrc...D....@.....@..@.rel oc.....`.....@..B.....!.....H.....x..$S.....U.....0.....(....(.....(.....o ...*.....(!.....("....(#.....($.....(%....*N..(....o.... (&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\OEpDLNVZW.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.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):	7.373755208458107
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
File size:	729088
MD5:	d765dcbdabed2ed1dd0fdd8800f221ed
SHA1:	be68fc678cca6434577d7af59abf129569ab7b47
SHA256:	d2693c3162e3ea906bf7fc546a07985a3bf55bbfb78f52015265cf7140eed31f
SHA512:	f4345f41a035c8d4502411a36001c4ee5a02d9f85f3fe00fc5dc97a7860470d545f9c0c1c1eec1633adcc391c1a326d6b4d3833e60c66a2de50cd7d170d335c2
SSDEEP:	12288:xClJbGEIGv5dKbr/Yy1V5LYRs5dCJ/ninKUGTSZ+gFQ6CYjcMfNsKcRJN8P:OJ7IogPHZY8KfTScKNjcMfXcOP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...PH4`.....P....."... ...@....@.. ....@.....

File Icon

Icon Hash:	e4a65d44a4aca8e4

Static PE Info

General

Entrypoint:	0x482206
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:	0x60344850 [Tue Feb 23 00:12:00 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

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
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	0x821b4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x84000	0x31644	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x8020c	0x80400	False	0.77356313962	data	7.49616773299	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x31644	0x31800	False	0.516867897727	data	6.6220959465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	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_ICON	0x842b0	0x8bf4	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x8cea4	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9d6cc	0x94a8	data		
RT_ICON	0xa6b74	0x5488	data		
RT_ICON	0xabffc	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 57599, next used block 4278648832		
RT_ICON	0xb0224	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb27cc	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 718597314, next used block 33554431		
RT_ICON	0xb3874	0x988	data		
RT_ICON	0xb41fc	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xb4664	0x84	data		
RT_VERSION	0xb46e8	0x34c	data		
RT_MANIFEST	0xb4a34	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	X509KeyStorageFlags.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	X509KeyStorageFlags.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:05:04.595701933 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.643071890 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.643220901 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.692361116 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.759031057 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.759613037 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.769243002 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.816570997 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.837476015 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.908401966 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.930315971 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.939142942 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.939169884 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.939187050 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.939203978 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.939217091 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.939294100 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.939311028 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.985728025 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985759020 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985774994 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985790014 CET	4837	49708	45.137.22.36	192.168.2.3

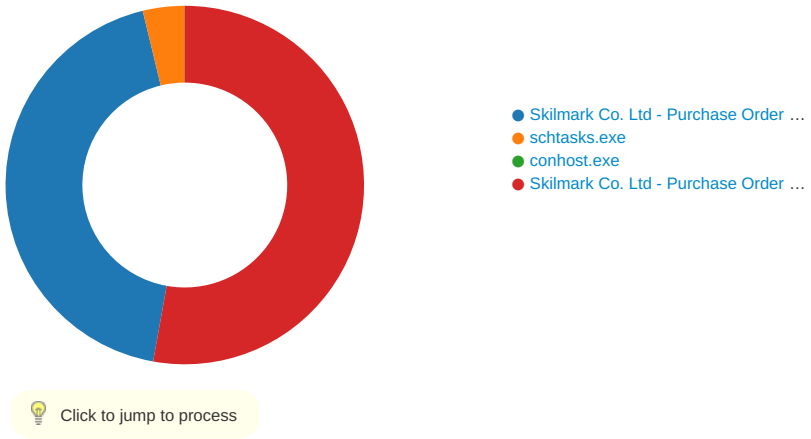
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:05:04.985804081 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985825062 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985841990 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985858917 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985863924 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.985872984 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:04.985888958 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:04.985919952 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032422066 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032444000 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032460928 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032478094 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032496929 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032505989 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032516003 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032533884 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032541990 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032551050 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032568932 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032569885 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032586098 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032604933 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032623053 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032641888 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032644033 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032659054 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032660961 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032669067 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.032680035 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032692909 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.032766104 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079194069 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079221010 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079236984 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079252005 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079268932 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079288006 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079308033 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079328060 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079344034 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079355955 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079361916 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079381943 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079401016 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079412937 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079418898 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079428911 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079437017 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079457045 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079476118 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079493046 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079509020 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079514027 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079525948 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079544067 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079559088 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079564095 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079576969 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079597950 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079607964 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079617023 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079617977 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079634905 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079651117 CET	4837	49708	45.137.22.36	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:05:05.079667091 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079683065 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079699039 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079715967 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079726934 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079734087 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.079754114 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.079917908 CET	49708	4837	192.168.2.3	45.137.22.36
Feb 23, 2021 09:05:05.126466036 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.126535892 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.126578093 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.126626015 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.126669884 CET	4837	49708	45.137.22.36	192.168.2.3
Feb 23, 2021 09:05:05.126698017 CET	49708	4837	192.168.2.3	45.137.22.36

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Skilmark Co. Ltd - Purchase Order 022021.pdf.exe PID: 6424 Parent PID: 5608

General

Start time:	09:04:41
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe'
Imagebase:	0xa70000
File size:	729088 bytes
MD5 hash:	D765DCBDABED2ED1DD0FDD8800F221ED
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: 00000000.00000002.254941968.0000000004113000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254941968.0000000004113000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254941968.0000000004113000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.253631018.0000000002EE2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.253583069.0000000002E91000.00000004.00000001.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	6E0CCF06	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	6E0CCF06	unknown
C:\Users\user\AppData\Roaming\OEpDLNVZW.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	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\OEpDLNVZW.exe\:Zone.Identifier :$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8B36.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8B36.tmp	success or wait	1	6CF16A95	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\OEpDLNVZW.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 50 48 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 04 08 00 00 1a 03 00 00 00 00 00 06 22 08 00 00 20 00 00 00 40 08 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 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...PH4`.......... ....P............."... ...@....@.. ....@................	success or wait	3	6CF1DD66	CopyFileW
C:\Users\user\AppData\Roaming\ OEpDLNVZW.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	6CF1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8B36.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/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CF11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E3DC907	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile

Analysis Process: schtasks.exe PID: 7004 Parent PID: 6424

General

Start time:	09:04:59
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OEpDLNVZW' /XML 'C:\Users\user\AppData\Local\Temp\tmp8B36.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\tmp8B36.tmp	unknown	2	success or wait	1	2AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8B36.tmp	unknown	1643	success or wait	1	2AABD9	ReadFile

Analysis Process: conhost.exe PID: 7012 Parent PID: 7004

General

Start time:	09:04:59
Start date:	23/02/2021
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: Skilmark Co. Ltd - Purchase Order 022021.pdf.exe PID: 7048 Parent PID: 6424

General

Start time:	09:05:00
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe
Imagebase:	0x8c0000
File size:	729088 bytes
MD5 hash:	D765DCBDABED2ED1DD0FDD8800F221ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6E0CCF06	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	6E0CCF06	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	6CF1BEFF	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	6CF11E60	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	6CF1BEFF	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	6CF1BEFF	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	15	6CF11E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF11E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF11E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe:Zone.Identifier	success or wait	1	6CE92935	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	95 2d 3f 29 1d d8 d8 48	.-?)...H	success or wait	1	6CF11B4F	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	8	6CF11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CF11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CF11B4F	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	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF11B4F	ReadFile
C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe	unknown	4096	success or wait	1	6E08D72F	unknown
C:\Users\user\Desktop\Skilmark Co. Ltd - Purchase Order 022021.pdf.exe	unknown	512	success or wait	1	6E08D72F	unknown

Disassembly

Code Analysis