ID: 385474
Sample Name: Purchase Order.exe
Cookbook: default.jbs
Time: 15:16:19
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

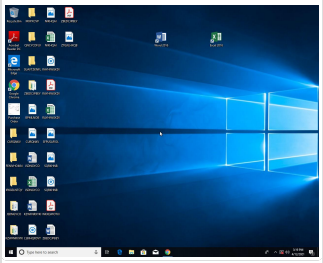
Analysis Report Purchase Order.exe

Overview

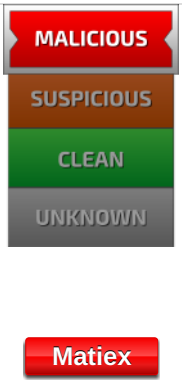
General Information

Sample Name:	Purchase Order.exe
Analysis ID:	385474
MD5:	4953a0238e7814..
SHA1:	006a605fa48b26b.
SHA256:	51688c6b77d1a0..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

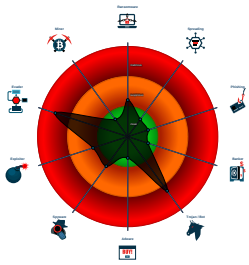


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected Matiex Keylogger
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…
- Yara detected Beds Obfuscator
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…
- Contains functionality to call native f…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Detected potential crypto function
- Enables debug privileges

Classification



Startup

- **System is w10x64**
- Purchase Order.exe (PID: 6632 cmdline: 'C:\Users\user\Desktop\Purchase Order.exe' MD5: 4953A0238E781408FAE3EE737BF14AC4)
  - Purchase Order.exe (PID: 6784 cmdline: C:\Users\user\Desktop\Purchase Order.exe MD5: 4953A0238E781408FAE3EE737BF14AC4)
    - dw20.exe (PID: 6824 cmdline: dw20.exe -x -s 748 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.427728679.000000000402000.00000040.00000001.sdmp	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
00000002.00000002.427728679.000000000402000.00000040.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000000.00000002.348990165.0000000002A0D000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.350207077.0000000003A8E000.00000004.00000001.sdmp	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
00000000.00000002.350207077.0000000003A8E000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	

Click to see the 5 entries

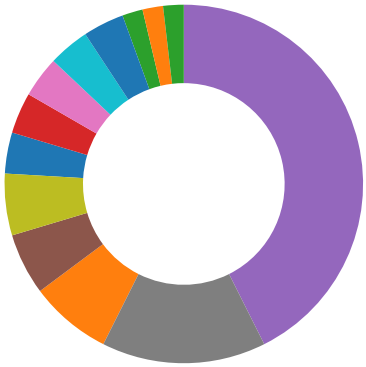
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Purchase Order.exe.3c71470.2.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
0.2.Purchase Order.exe.3c71470.2.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
2.2.Purchase Order.exe.4228d4.1.raw.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
2.2.Purchase Order.exe.4228d4.1.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
2.2.Purchase Order.exe.400000.0.unpack	JoeSecurity_Matiex	Yara detected Matiex Keylogger	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- 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:

Multi AV Scanner detection for submitted file

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected Beds Obfuscator

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Matiex Keylogger

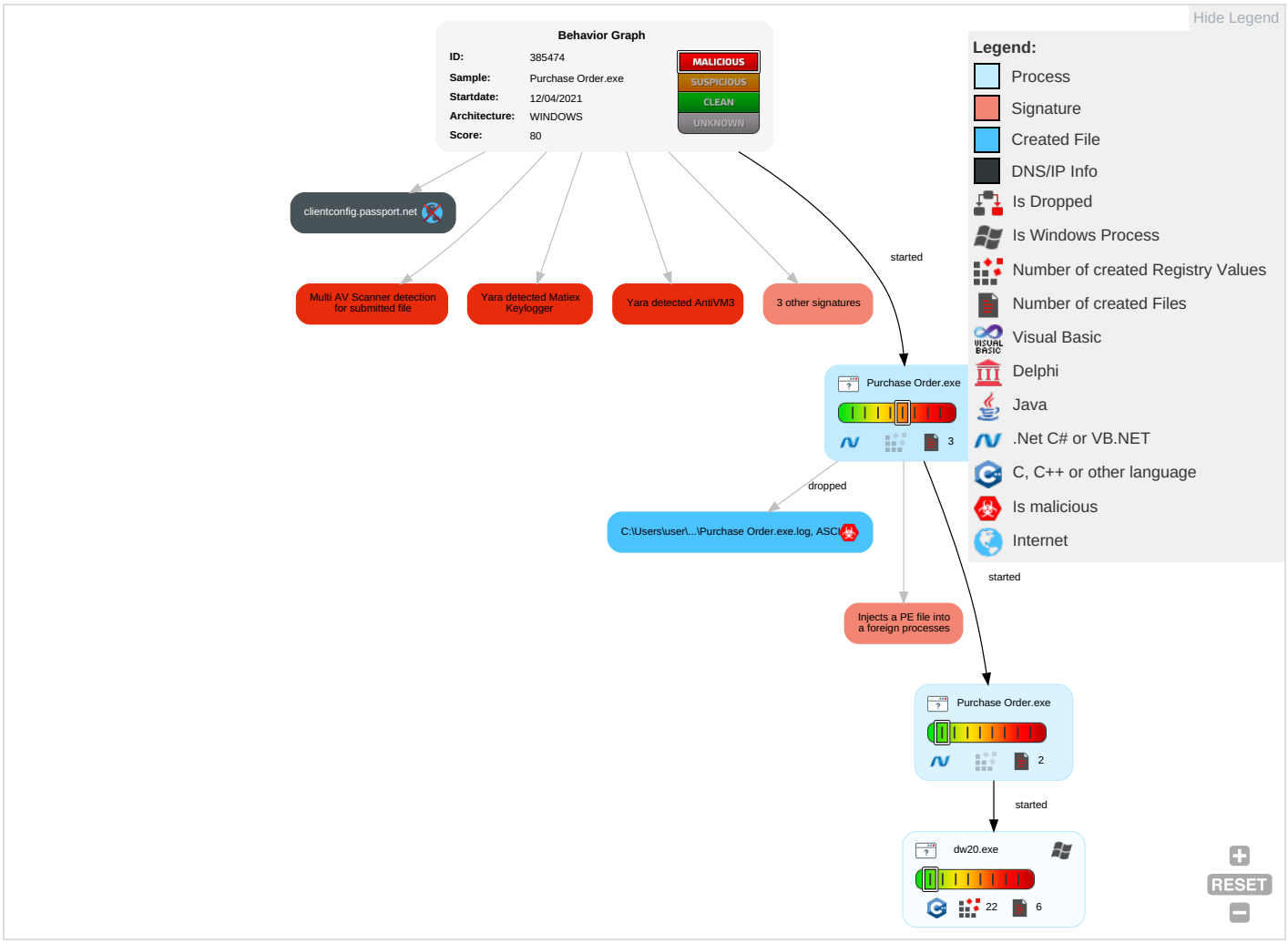
Remote Access Functionality:

Yara detected Matiex Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

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
Purchase Order.exe	35%	Virustotal		Browse
Purchase Order.exe	19%	Metadefender		Browse
Purchase Order.exe	48%	ReversingLabs	ByteCode-MSIL.Infostealer.Coins	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Purchase Order.exe.400000.0.unpack	100%	Avira	TR/Redcap.jajcu		Download File

Domains

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

URLs

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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comdiaa3W	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://weather.gc.ca/astro/seeing_e.html)	0%	Avira URL Cloud	safe	
http://www.carterandcone.com4	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comldva	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.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.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.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/NW	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.como.M	0%	Avira URL Cloud	safe	
http://www.carterandcone.comlt	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnueGZ	0%	Avira URL Cloud	safe	
http://www.carterandcone.comCf	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cne	0%	Avira URL Cloud	safe	
http://www.carterandcone.comg	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comk	0%	URL Reputation	safe	
http://www.carterandcone.comle	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/ita	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cndkW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clientconfig.passport.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html8	Purchase Order.exe, 00000000.00000003.330299371.0000000004DB5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comdiaa3W	Purchase Order.exe, 00000000.00000003.347164147.0000000004D80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp, Purchase Order.exe, 00000000.00000003.324401456.0000000004D9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://weather.gc.ca/astro/seeing_e.html)	Purchase Order.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp, Purchase Order.exe, 00000000.00000003.347164147.0000000004D80000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com4	Purchase Order.exe, 00000000.00000003.326857154.0000000004D85000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Purchase Order.exe, 00000000.00000003.326857154.0000000004D85000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Purchase Order.exe, 00000000.00000002.348990165.0000000002A0D000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com.	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comldva	Purchase Order.exe, 00000000.00000003.347164147.0000000004D80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp, Purchase Order.exe, 00000000.00000003.327836247.0000000004DB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Purchase Order.exe, 00000000.00000003.331404936.0000000004DB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.agfamonotype.	Purchase Order.exe, 00000000.00000003.329870889.0000000004DB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/NW	Purchase Order.exe, 00000000.00000003.327278693.0000000004D88000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.M	Purchase Order.exe, 00000000.00000003.326857154.0000000004D85000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comlt	Purchase Order.exe, 00000000.00000003.326857154.0000000004D85000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnueGZ	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comCf	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cne	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comg	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	Purchase Order.exe, 00000000.00000003.326857154.0000000004D85000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comk	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comle	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Purchase Order.exe, 00000000.00000003.329870889.0000000004DB5000.00000004.00000001.sdmp, Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp, Purchase Order.exe, 00000000.00000003.327278693.0000000004D88000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ita	Purchase Order.exe, 00000000.00000003.327278693.0000000004D88000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Purchase Order.exe, 00000000.00000002.355094483.0000000004F92000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cndkW	Purchase Order.exe, 00000000.00000003.326231503.0000000004D86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/e	Purchase Order.exe, 00000000.00000003.327278693.0000000004D88000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/d	Purchase Order.exe, 00000000.00000003.327278693.0000000004D88000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385474

Start date:	12.04.2021
Start time:	15:16:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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:	mal80.troj.evad.winEXE@5/4@1/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.6% (good quality ratio 2.8%) • Quality average: 33.4% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 81% • 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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, wermgr.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 2.23.155.232, 2.23.155.186, 20.50.102.62, 88.221.62.148, 92.123.150.225, 92.122.213.194, 92.122.213.247, 13.88.21.125, 52.155.217.156, 20.54.26.129, 92.122.144.200 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, a767.dspw65.akamai.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, authgfx.msa.akadns6.net, go.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, download.windowsupdate.com, download.windowsupdate.com.edgesuite.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:17:15	API Interceptor	1x Sleep call for process: Purchase Order.exe modified
15:17:57	API Interceptor	1x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Purchase Order.e_f38b3ed14dba9e7d30b75ea9b7736a5b21d8e31f_00000000_1afbc56f\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10158
Entropy (8bit):	3.7633564412815135
Encrypted:	false
SSDEEP:	96:CyenOSA/0zxWs5h5pXI/+BHUHZopAnQ0DFH2EmSonj+wdOyWnEeVc1F9ZQb5iMFH:xenOgDHvaPLk9Mn/u7sNS274ItF
MD5:	EDC36D4D4D275A2B46249E2AA6CBE55E
SHA1:	CE36456426E58D96F323193F6F7460D1C6DF29FD
SHA-256:	43C54784D385E90B057C8EC509CCDA80BBBDC682881ABA512350D59A223FF660
SHA-512:	FFD703F69DDE2300B11527CEBB7A808B76CB14FECD45AAA8FD185C3229D5E262AF84B0EE7E53FB5F0FB77201F12102FAB2A637927652AA40576BA0AB0C82B0CC
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.7.3.9.4.4.1.6.4.5.9.7.2.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.7.3.9.4.4.3.8.9.5.9.6.1.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.3.4.c.9.f.7.f.-.8.4.c.1.-.4.8.6.d.-.a.1.9.0.-.e.8.2.7.9.8.6.2.2.1.4.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.A.s.s.e.m.b.l.y.N.a.m.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.8.0.-.0.0.0.1.-.0.0.1.7.-.3.4.c.5.-.2.f.9.a.e.9.2.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.a.b.f.0.9.a.7.d.4.c.1.1.e.2.7.b.a.7.0.b.c.3.0.f.a.2.d.6.c.a.0.0.0.0.0.0.0.0.0.0.!.0.0.0.0.0.6.a.6.0.5.f.a.4.8.b.2.6.b.2.7.e.8.5.9.c.0.3.1.3.4.0.3.4.4.9.3.7.8.5.8.3.9.8.!.P.u.r.c.h.a.s.e. .O.r.d.e.r...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.4././.1.1.:.1.5.:.5.8.:.5.9.!.0.!.P.u.r.c.h.a.s.e. .O.r.d.e.r...e.x.e.....B.o.o.t.I.d.=.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C9.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7624
Entropy (8bit):	3.7001256134003873
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiA+G6bgB6YU+56IgmfkT8SwCp15D1flTm:RrlsNiY6bgB6Yj6IgmfkYSZ5xfM
MD5:	5485A5684E2E126255D69664087FA626
SHA1:	AB9F71D28E5277EC7844E55A368235DF292D1AA6
SHA-256:	B57AF341EAAC6AE884AE2CC577B34DF4794A1BB524E299531D1294B396A97752
SHA-512:	F2B54944402CD6C9510542003D56622D056B7877BCF3971A3B6A341CBA2865A58B9C512012BF263534F36292A130D3296525BCDB77FAAE7CDE4470F1AB1DC2F0
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3AC4.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4614
Entropy (8bit):	4.484824980131556
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9qUWSC8BCTM8fm8M4JFKf5vNJoFpvX+q8dB6saq+QIeO1VOd:uITfQBNSNUJFKRjqvX+YTqDxMOd
MD5:	805AA8E5719DA0E01DF875EA504F3165

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3AC4.tmp.xml	
SHA1:	CB1AF469E3B11D07D6F89DDC7CDC3E6D667F3DF0
SHA-256:	26FD6FD2682CFBB4AA36E13E8B930D164C539141F6405F63BC27085B702DED68
SHA-512:	9DB71DE84D0847CC4AD4F541F7E50D46BDAF9B000E680FA5BEEC70225D81A7C25953B509D0831E936A6540EDADE3879AA622B9CEFAE4938B22BD98D5BCEDE0C4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="943648" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Purchase Order.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.40598591003729
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:	Purchase Order.exe
File size:	826368
MD5:	4953a0238e781408fae3ee737bf14ac4
SHA1:	006a605fa48b26b27e859c031340344937858398
SHA256:	51688c6b77d1a093fc0d9efe21413f09d1bfef7907a726e8498e2173abb7c8d4
SHA512:	57920e2f67b62c443eb3f5319697b75d892df7a78a04f330f00aae8b821714719d2a2af1bec849765effc4df64f8ddf0bed4ed3cf81005cbcc7fff46cfd1d3c7
SSDEEP:	12288:LDlXerqEw/rZm+ZoF2pYGIZv4LYSdSC3I7GwPP5qRzYjJsa9ODrmOzvZ1+fLI/LE:LDderqn/w+/pYFvRC3I7GPc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..N...L.....I.. .....@.. .....@.....

File Icon

	
Icon Hash:	4125655370600101

Static PE Info

General

Entrypoint:	0x4c6cae
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:	0x60731CC3 [Sun Apr 11 15:58:59 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc6c54	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x4928	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	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	0xc4cb4	0xc4e00	False	0.751769593254	data	7.4406354621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x4928	0x4a00	False	0.152502111486	data	2.63585312657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	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	0xc8130	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0xcc358	0x14	data		
RT_VERSION	0xcc36c	0x3d0	data		
RT_MANIFEST	0xcc73c	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 CodeUnit 2007
Assembly Version	2007.8.28.1
InternalName	AssemblyName.exe
FileVersion	2007.08.28.1
CompanyName	CodeUnit
LegalTrademarks	
Comments	Image Size Standardiser
ProductName	Image Size Standardiser
ProductVersion	2007.08.28.1
FileDescription	Image Size Standardiser
OriginalFilename	AssemblyName.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-15:17:09.781420	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:09.816438	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/12/21-15:17:09.822526	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:09.859114	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
04/12/21-15:17:09.859602	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:09.897177	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.50.25	192.168.2.6
04/12/21-15:17:09.901722	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:09.942778	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.62	192.168.2.6
04/12/21-15:17:09.963919	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:10.011057	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.253	192.168.2.6
04/12/21-15:17:10.019437	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:10.065968	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.14.78	192.168.2.6
04/12/21-15:17:10.075882	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:10.137518	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.117	192.168.2.6
04/12/21-15:17:10.143003	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:10.196196	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
04/12/21-15:17:10.197569	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-15:17:10.250018	ICMP	408	ICMP Echo Reply			2.23.155.232	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:17:02.188210964 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:02.237078905 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:03.432223082 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:03.483798981 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:05.396575928 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:05.454792976 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:06.678920031 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:06.727936029 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:07.545471907 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:07.594119072 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:08.694360971 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:08.745882988 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:09.714747906 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:09.778441906 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:22.027512074 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:22.076325893 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:26.153947115 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:26.211657047 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:26.593698025 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:26.642446995 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:27.371833086 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:27.420711994 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:34.325079918 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:34.376645088 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:34.408814907 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:34.470855951 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:34.708123922 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:34.768985033 CEST	53	63745	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:17:36.268973112 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:36.318243027 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:37.055372000 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:37.104171991 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:38.166023970 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:38.214950085 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:39.136960983 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:39.204515934 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:39.843059063 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:39.892381907 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:40.965179920 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:41.013802052 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:45.238478899 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:45.290182114 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:46.344132900 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:46.392785072 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:48.259892941 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:48.311598063 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:56.168281078 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:56.395606041 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:56.946171999 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:57.099788904 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:57.658051014 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:57.671370029 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:57.728770018 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:57.732328892 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:58.474102974 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:58.578263044 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:59.118072033 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:59.177898884 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 15:17:59.320744991 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:17:59.369261026 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:00.133456945 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:00.193588018 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:00.746002913 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:00.805965900 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:01.914160013 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:02.109582901 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:03.823339939 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:03.884013891 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:04.328334093 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:04.377125978 CEST	53	56129	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:10.531311989 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:10.589813948 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:41.917402029 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:41.985662937 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:42.723320961 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:42.772187948 CEST	53	54069	8.8.8.8	192.168.2.6
Apr 12, 2021 15:18:44.454745054 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 12, 2021 15:18:44.512132883 CEST	53	61178	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:17:34.708123922 CEST	192.168.2.6	8.8.8.8	0x73a6	Standard query (0)	clientconf ig.passport.net	A (IP address)	IN (0x0001)

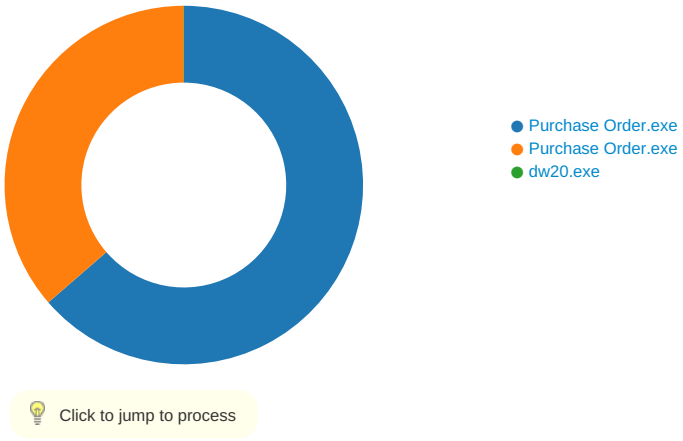
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:17:34.768985033 CEST	8.8.8.8	192.168.2.6	0x73a6	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase Order.exe PID: 6632 Parent PID: 5956

General

Start time:	15:17:07
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order.exe'
Imagebase:	0x320000
File size:	826368 bytes
MD5 hash:	4953A0238E781408FAE3EE737BF14AC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.348990165.0000000002A0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000000.00000002.350207077.0000000003A8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.350207077.0000000003A8E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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\Local\Microsoft\CLR_v2.0_32\UsageLogs\Purchase Order.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Purchase Order.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: Purchase Order.exe PID: 6784 Parent PID: 6632

General

Start time:	15:17:19
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order.exe

Imagebase:	0xe70000
File size:	826368 bytes
MD5 hash:	4953A0238E781408FAE3EE737BF14AC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Matiex, Description: Yara detected Matiex Keylogger, Source: 00000002.00000002.427728679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000002.00000002.427728679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

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

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

Analysis Process: dw20.exe PID: 6824 Parent PID: 6784

General

Start time:	15:17:20
Start date:	12/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 748
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis