ID: 321085
Sample Name: Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe
Cookbook: default.jbs
Time: 10:56:58
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
Anti Debugging: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 12
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 14
IPs 14
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 18
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18

Entrypoint Preview 18
Data Directories 19
Sections 20
Resources 20
Imports 20
Version Infos 20
Possible Origin 20
Network Behavior 20
TCP Packets 20
UDP Packets 22
DNS Queries 23
DNS Answers 23
HTTP Request Dependency Graph 24
HTTP Packets 24
HTTPS Packets 25
Code Manipulations 25
User Modules 25
Hook Summary 25
Processes 25
Statistics 25
Behavior 25
System Behavior 26
Analysis Process: Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe PID: 6304 Parent PID: 5868 26
General 26
File Activities 26
Analysis Process: Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe PID: 6780 Parent PID: 6304 26
General 26
File Activities 27
File Created 27
File Read 27
Analysis Process: explorer.exe PID: 3424 Parent PID: 6780 27
General 27
File Activities 27
Analysis Process: cmstp.exe PID: 6004 Parent PID: 3424 28
General 28
File Activities 28
File Read 28
Analysis Process: cmd.exe PID: 2108 Parent PID: 6004 28
General 28
File Activities 29
File Deleted 29
Analysis Process: conhost.exe PID: 2860 Parent PID: 2108 29
General 29
Disassembly 29
Code Analysis 29

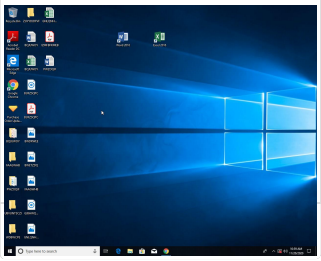
Analysis Report Purchase Order Updates thyssenkrupp…

Overview

General Information

Sample Name:	Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe
Analysis ID:	321085
MD5:	6008cd180e677b..
SHA1:	881844503dee7d..
SHA256:	b8b07584a493c3..
Tags:	exe GuLoader

Most interesting Screenshot:



Detection

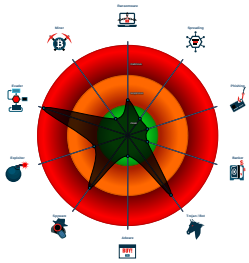
FormBook GuLoader

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe (PID: 6304 cmdline: 'C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe' MD5: 6008CD180E677BE4846D5F8ABFA6B983)
  - Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe (PID: 6780 cmdline: 'C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe' MD5: 6008CD180E677BE4846D5F8ABFA6B983)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 6004 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 2108 cmdline: /c del 'C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

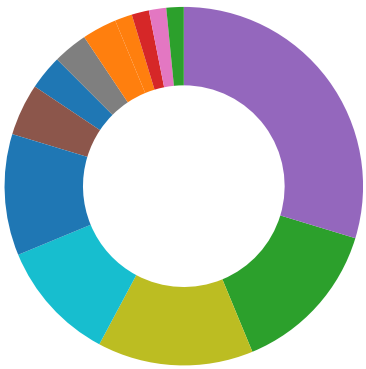
Source	Rule	Description	Author	Strings
00000006.00000002.921168798.0000000002E40000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.921168798.0000000002E40000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b307:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c30a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.921168798.0000000002E40000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183e9:$sqlite3step: 68 34 1C 7B E1 • 0x184fc:$sqlite3step: 68 34 1C 7B E1 • 0x18418:$sqlite3text: 68 38 2A 90 C5 • 0x1853d:$sqlite3text: 68 38 2A 90 C5 • 0x1842b:$sqlite3blob: 68 53 D8 7F 8C • 0x18553:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.920987753.0000000002960000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.920987753.0000000002960000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b307:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c30a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Yara detected Generic Dropper

Remote Access Functionality:

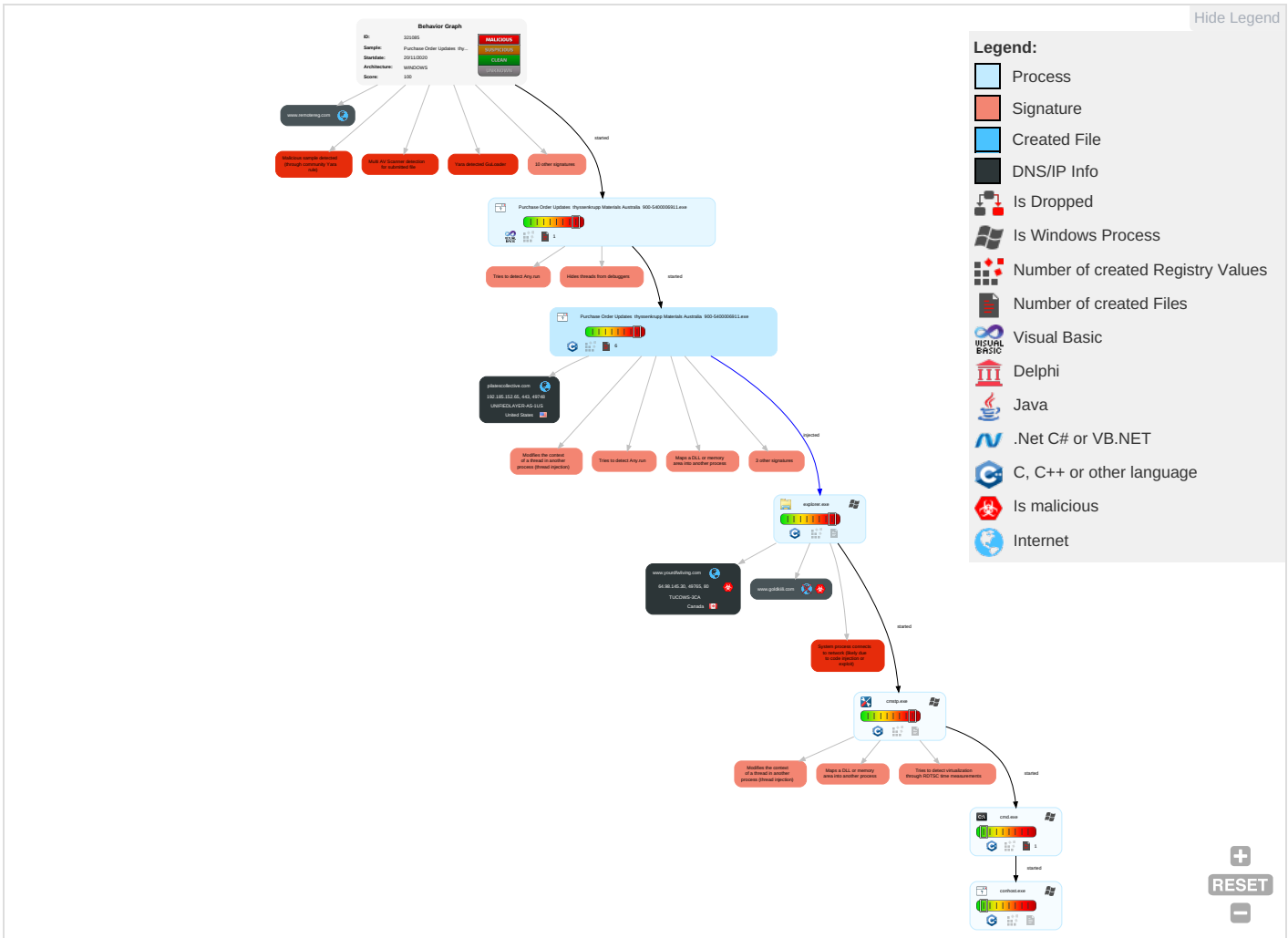
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 6 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Information Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

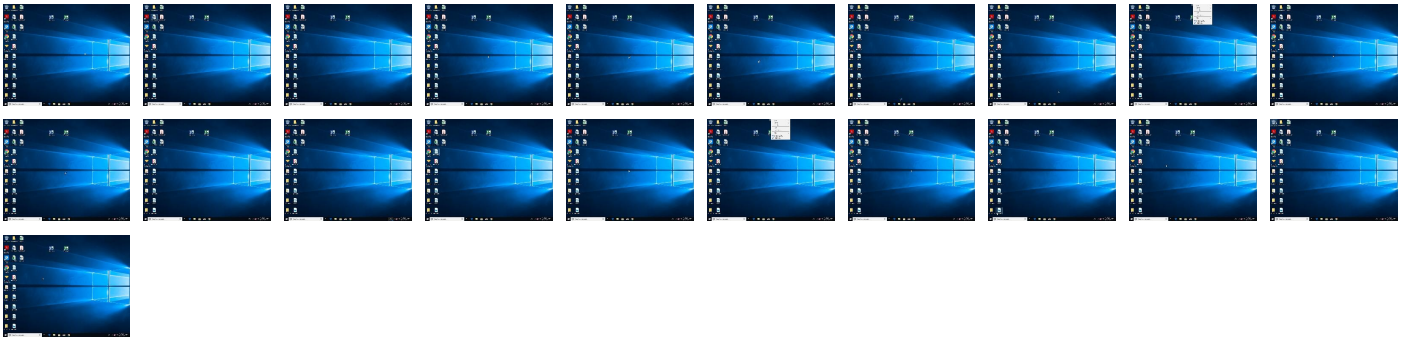
Behavior Graph



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 Updates thyssenkrupp Materials Australia 900-5400006911.exe	31%	Virustotal		Browse
Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe	15%	ReversingLabs	Win32.Trojan.Bulz	

Dropped Files

No Antivirus matches

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	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.yourdfwliving.com/ca5e/?9rmT0Zz8=33d4ALcEm9QS3ETZfm99n5/91vkYSjLj82bPV1gW1bkPYk/ky+qZQnI1oXWMSZEPGOwK&rZ=Xn8pd6vp	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.goodfont.co.kr	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.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.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.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/	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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.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.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.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.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pilatescollective.com	192.185.152.65	true	false		high
www.yourdfwliving.com	64.98.145.30	true	true		unknown
www.remotereg.com	45.79.19.196	true	false		unknown
www.goldkiili.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.yourdfwliving.com/ca5e/?9rmT0Zz8=33d4ALcEm9QS3ETZfm99n5/91vkYSjLj82bPV1gW1bkPYk/ky+qZQnI1oXWMSZEPGOwK&rZ=Xn8pd6vp	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hover.com/domain_pricing?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://https://www.hover.com/privacy?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://https://twitter.com/hover	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/hover_domains	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hover.com/transfer_in?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hover.com/renew?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://https://pilatescollective.com/myguy/anyiba_ivtYLdKxk45.bin	Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe, 00000001.00000002.757436469.0000000000563000.00000040.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hover.com/email?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://https://www.hover.com/about?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://https://www.hover.com/domains/results	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://https://www.hover.com/tos?source=parked	cmstp.exe, 00000006.00000002.922184165.00000000054EF000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.00000000.741826689.000000000B976000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.00000000.720261715.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	explorer.exe, 00000004.0000000 0.741826689.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.741826689.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.741826689.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.741826689.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.741826689.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hover.com/tools?source=parked	cmstp.exe, 00000006.00000002.9 22184165.00000000054EF000.0000 0004.00000001.sdmp	false		high
http://https://help.hover.com/home?source=parked	cmstp.exe, 00000006.00000002.9 22184165.00000000054EF000.0000 0004.00000001.sdmp	false		high
http://https://www.hover.com/?source=parked	cmstp.exe, 00000006.00000002.9 22184165.00000000054EF000.0000 0004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.98.145.30	unknown	Canada		32491	TUCOWS-3CA	true
192.185.152.65	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321085
Start date:	20.11.2020
Start time:	10:56:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/0@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.7% (good quality ratio 21.3%) • Quality average: 68.8% • Quality standard deviation: 33.8%
HCA Information:	• Successful, ratio: 94% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 13.64.90.137, 51.104.144.132, 52.155.217.156, 20.54.26.129, 95.101.22.134, 95.101.22.125 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
64.98.145.30	u8u7GG8XMY.exe	Get hash	malicious	Browse	• www.sympubs.com/sub/?1b=jlNDpL_hl&adsdULx=exbU4/4dWJb0lwCgUWABnYfjcMy2h9OMC/Y2efpEd3U5UcjGsPJLwYDLgnBBw3TFDQbKcpVMBA==
	qpFvMReV7S.exe	Get hash	malicious	Browse	• www.iuvo.xyz/d9s8/?t8o=he92EdQzs/Hz/UE/j8/qY0GgF1dsuDtJC9/WaaPYDs9hWFm06jox2nFyIpmHj3SNb2Wg8n6Qjg==&Tj=YpIp
	mp0nMsMroT.exe	Get hash	malicious	Browse	• www.homecaredispatch.com/0tog/?K8ePY=0HRdnbOcFNnxvyqGcVRvrrLsbqQ9r15luAj7Zds+T+sucbkdrSSKiOrsMjTBx8eXU9lb&uTrL=ArghXbG
	request for quotation and samples Nos 0708090504 0 692168035 0567034016 0607089403 0506079436.exe	Get hash	malicious	Browse	• www.bridgecounsel.com/iwnn/?VV=I4Wln9W2K08RsgFTS7xOtS0lo2xQAdJXy6pSooKD6GidwymYIEze67OEiKijrMdb1Oql&2d=YnaxWrUh
	Packing list Q950.exe	Get hash	malicious	Browse	• www.firesideeditions.com/hnh/?GTg0=16n/EVTVvrPY03ZM1cgxu8vF+lz8aJHHZ9Ay32lZOf9jyEbegt6puRPXpTfetTqdkePI&5ju=UnSp
	900821.exe	Get hash	malicious	Browse	• harnessdog.com/robots.txt
	75employees -139-.js	Get hash	malicious	Browse	• www.briarhurst.org/2mo9u
	_output799FDD0.ex.exe	Get hash	malicious	Browse	• www.brocksquire.com/ph/?3fr4LdJ0=92v49/hxfXckg6seImwY8POmObuK+CZIvd5eySkU5X5K6iuwzcyW5QnNCYDBvgbiXqe9XdPIEwA827zstlH0Sg==&6lK=wv1p0l4Hq8mPL6F

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	68tt payment slip.exe	Get hash	malicious	Browse	• www.bgbhinc.com/ju/
	76Payment Confirmation.exe	Get hash	malicious	Browse	• www.bgbhinc.com/ju/
	29Sales Contract.exe	Get hash	malicious	Browse	• www.makesyougreat.com/m54/
	dana_attack_com_fil.exe	Get hash	malicious	Browse	• www.nocial-media.com/chu20/?3fg46tu=dulvafqgC+BqmqemqgY5WokFFUy91ErfkCX1z4wJ6S1QPFdLblH1G/D6178tlYfdHR3KZJqSc5TwZpL3JiSELg==&6lOL=v6Qlf8exdfOhQvQ
	user78698.7ci.ru	Get hash	malicious	Browse	• demosthenes.info/assets/images/polina.jpg
	MAOiAcNHG.exe	Get hash	malicious	Browse	• losangelesstreetsweeping.com/private/?5jUTGX5=L6KgL7JOpV7FIj6EBiwYaRf0tjW+r6xHLGD0GCrUSLDarW7yz9p+3hiUUYG/8MefkU3vYUTDP03GiHder38NIw==&t2Kde=3f0P0L&sql=1
	RF#Q20182401 ORDER N#Ub010014 New Supplier_PDF.exe	Get hash	malicious	Browse	• www.podimation.com/ax1/?00x=td1cEhBbeo8Rub8g9LhaiwGCB6q3SASHhirEgQDJ0fmdxXWHQ4LxN4J2ujarhZshQmQ/vqjjZVRlj+CwRDPADA==&4hp=7nTpgdD0x0eT
	3copy2.exe	Get hash	malicious	Browse	• www.fashionwalkoff.com/sb/?7nT=k5sb1Od/dqAl0xg6gy9dtqNiaaHfZk5L18HqEON64biWpkY5TYpTryyKKGJN+yS3gBUn+or2gdS01Zyu4y63Fg==&3fu4=pJeDbt2xRRpdaBY
	PO#A1218900.exe	Get hash	malicious	Browse	• www.goodorganicfood.online/ok/?id=gzLBHx8TS+wtmj3u7lpXCNGRFP9vqOythMn6UC4PS/lQEg8VoOhNwKe4U0pqYzFITbvLLjHXEzcjmrzk&pd=6lyL8bm
	www.unitedcpbocaraton.com	Get hash	malicious	Browse	• www.unitedcpbocaraton.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	www.unitedcpbocaraton.com	Get hash	malicious	Browse	• www.unitedcpbocaraton.com/
	77VLMDUET.exeDPKAA.exe	Get hash	malicious	Browse	• www.chickenstrings.com/cu/?4hUTBR=zidyfrKC1sXl5I7bAg8u3vPhhhl8xiuKJpDozSiMnQV9u8/igN2PQskIO/OqzIBewb8CIfjljZrQpykD30+eug==&w0Hl=3f3DUf
192.185.152.65	TR-D45.pdf.exe	Get hash	malicious	Browse	
	order.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pilatescollective.com	TR-D45.pdf.exe	Get hash	malicious	Browse	• 192.185.152.65
	order.exe	Get hash	malicious	Browse	• 192.185.152.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TUCOWS-3CA	u8u7GG8XMY.exe	Get hash	malicious	Browse	• 64.98.145.30
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 64.98.145.30
	8miw6WNHCt.exe	Get hash	malicious	Browse	• 64.98.36.4
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 64.98.145.30
	lQtvZjIdhN.exe	Get hash	malicious	Browse	• 64.98.145.30
	148wWoi8vI.exe	Get hash	malicious	Browse	• 64.98.145.30
	qpFvMReV7S.exe	Get hash	malicious	Browse	• 64.98.145.30
	G8CACnQy05.exe	Get hash	malicious	Browse	• 64.98.36.128
	mp0nMsMroT.exe	Get hash	malicious	Browse	• 64.98.145.30
	8QnG43d6KO.exe	Get hash	malicious	Browse	• 64.98.36.128
	AUGUST_INVOICE_COPIES.xls	Get hash	malicious	Browse	• 64.98.36.128
	SecuriteInfo.com.CAP_HookExKeylogger.20427.exe	Get hash	malicious	Browse	• 64.98.36.128
	Product-scample072.exe	Get hash	malicious	Browse	• 64.98.36.128
	Invoice-Copies_May_Aug.xls	Get hash	malicious	Browse	• 64.98.36.128
	request for quotation and samples Nos 0708090504 0 692168035 0567034016 0607089403 0506079436.exe	Get hash	malicious	Browse	• 64.98.145.30
	Packing list Q950.exe	Get hash	malicious	Browse	• 64.98.145.30
UNIFIEDLAYER-AS-1US	TR-D45.pdf.exe	Get hash	malicious	Browse	• 192.185.152.65
	Shipping Documents (INV,PL,BL)_pdf.exe	Get hash	malicious	Browse	• 192.185.170.106
	Information-822908953.doc	Get hash	malicious	Browse	• 192.232.229.53
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 162.241.67.201
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 162.241.67.195
	http://https://app.box.com/s/gdf36roak3w2fc52cgfbxuq651p0zehy	Get hash	malicious	Browse	• 162.241.87.44
	ef5ai1p.dll	Get hash	malicious	Browse	• 192.232.229.53
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 192.254.236.192
	Documentation.478396766.doc	Get hash	malicious	Browse	• 192.232.229.53
	order.exe	Get hash	malicious	Browse	• 192.185.152.65
	Documentation.478396766.doc	Get hash	malicious	Browse	• 162.241.44.26
	8OP0MEmSDd.dll	Get hash	malicious	Browse	• 192.232.229.53
	Information-478224510.doc	Get hash	malicious	Browse	• 192.232.229.53
	ZcmAPc4xeE.dll	Get hash	malicious	Browse	• 162.241.44.26
	7aKeSIV5Cu.dll	Get hash	malicious	Browse	• 192.232.229.53
	qRMGCk1u96.dll	Get hash	malicious	Browse	• 192.232.229.53
	qAm7u8G4lM.exe	Get hash	malicious	Browse	• 192.185.138.193
	AWB# 9284730932.exe	Get hash	malicious	Browse	• 192.185.170.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Document3327.xlsb	Get hash	malicious	Browse	• 198.57.244.39
	POSH XANADU Order-SP-20093000-xlxs.xlsx	Get hash	malicious	Browse	• 192.185.144.204

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	http://https://u19114248.ct.sendgrid.net/ls/click?upn=1kMFt-2Foese19BdzKqBBNxmUiDNiO3l4ozyKR3JHYHjGXyXtR1YgfLizwybC7hwFoy4wlb-2FUZczInc9Ssmzz4dQ-3D-3DuU6r_TCf26aIMQHFUMJSqtVnzlcWBqfQpkiFxCOBj9heiSevnqRkiapxQjkatt3r5u5xw-2FNDgXhA220pIRwcKmyMneET98pBkuhL-2FUwJCaSrvE5mZhnMBtJdZf9Opljklq5t7Y-2BINqElPlJU8bjYLY27qV6L-2FSwA36husfmMqwKagSwOgE04FdniEmY9uEbym50XNhqKw9lgczv6HrSrYNm6ouXnIayW-2FSBLzGYxoTYKe6OA-3D	Get hash	malicious	Browse	• 192.185.152.65
	http://https://rugbysacele.ro/zz/IK/of1/nhctfwp4x278qkbusvijl6z39y5ema1o0gdr597irqhw4x0fk3uevzlaoj12bdmpsnt8g6yce40h6iv7bprsowxd3z2nmu8kal5gcj1yf9qt?data=dmluY2VudC5kdXNvcmRldEBpbWQub3Jn#aHR0cHM6Ly9ydWdieXNhY2VsZS5yby96ei9JSy9vZjEvNDUzMjY3NzY4JmVtYWlsPXZpbmNlbnQuZHVzb3JkZXRAaW1kLm9yZw==	Get hash	malicious	Browse	• 192.185.152.65
	TR-D45.pdf.exe	Get hash	malicious	Browse	• 192.185.152.65
	Shipping Documents (INV,PL,BL)_pdf.exe	Get hash	malicious	Browse	• 192.185.152.65
	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 192.185.152.65
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 192.185.152.65
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 192.185.152.65
	http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 192.185.152.65
	http://https://bit.ly/2UDM1To	Get hash	malicious	Browse	• 192.185.152.65
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 192.185.152.65
	order.exe	Get hash	malicious	Browse	• 192.185.152.65
	http://45.95.168.116	Get hash	malicious	Browse	• 192.185.152.65
	http://https://u7342898.ct.sendgrid.net/ls/click?upn=HCSlWZDf9Xl-2FB6XFKqg1zjEMCja-2BnYJ5hRYKkDjy2dSVqjHsLlv5ZMXJXnh9JLSzwabeBrvYMnX699odsYkKotv4jgW-2BTippSHf276Hpn3fz0kcusnYHGKND7vKQPAS7g42-2FTb5zb8CNq57r3z9llg-3D-3DWdrE_hNl5WjNXy0NQcJb9Wql7qh7uPLeU7UGDRahFCFKbQLS6qwym7zJ-2B-2BhWsSSLs8pHa1w9VDlWPsA7ahHsZZucjX2ktFkSy5vhVZT2L3Jxh6b-2FoboCHa2CJGLfF19s71-2FI3WPC7rECe-2BEO9fLwbfggsNq2V1-2FqgMhzgJQL411ZuD7Y8pECisPKLf0vf9WvB1fyVO9o6Euui31Jg3e-2FDialpg2CbkM21Us8J-2FBk13yWzh58-3D	Get hash	malicious	Browse	• 192.185.152.65
	http://https://carolearmstrongrealestate.com/wpe/14ea332d0684051d9fef033a5f1607dd?usr=cnBlbmRsZXRvbkBkYXRlc3dlaXNlci5jb20=	Get hash	malicious	Browse	• 192.185.152.65
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 192.185.152.65
	http://https://prod.dfg152.ru/activate?key=23696252760045174930	Get hash	malicious	Browse	• 192.185.152.65
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 192.185.152.65
	BYRkah8GsZ.exe	Get hash	malicious	Browse	• 192.185.152.65
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 192.185.152.65
	splwow64.exe	Get hash	malicious	Browse	• 192.185.152.65

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.7572459878206415
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe
File size:	86016
MD5:	6008cd180e677be4846d5f8abfa6b983
SHA1:	881844503dee7d1797ce7736786dfec08f06100a
SHA256:	b8b07584a493c32a6f045b8bfe1f7ce2a2e441035a7048e946aa6b26a6485c0d
SHA512:	253fc6deeeb5647f9332412f3b0003b161736baa97cebe96149169bb5b9013c28f3850bd0a53181a8c23d5a1f72c755baaf2339af037b6c0760ad1e18aecfa1d
SSDEEP:	768:Mteyg1/gcK/WS3zWfxPSCFEI80v0dEeMTGUdP2KohBS:+eysgcK/WS36fxP/gEjPyhA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L..."._..... .....@.....`..... ....@.....

File Icon

	
Icon Hash:	00d6d4ec71b24430

Static PE Info

General

Entrypoint:	0x401360
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FB6BC22 [Thu Nov 19 18:40:34 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	0cb4f4ece3f5875b40d2bf4babdf78ef

Entrypoint Preview

Instruction
push 00403960h

Instruction
call 00007F0468A2AEA5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edi+edi*4], dh
mov byte ptr [1CFD67DEh], al
inc esi
mov bh, 4Bh
mov ah, D8h
cmp ebx, dword ptr [edx+0000007Ch]
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], ah
and byte ptr [eax], ah
and byte ptr [eax], ah
and byte ptr [ebp+63h], cl
popad
outsb
outsd
jc 00007F0468A2AF1Bh
arpl word ptr [eax], ax
jne 00007F0468A2AF14h
je 00007F0468A2AF24h
popad
push 00000000h
dec esp
xor dword ptr [eax], eax
add dword ptr [edi], esp
popad
pop ss
inc ebp
push esi
ror byte ptr [edi], 1
dec ecx
mov ch, B1h
jns 00007F0468A2AEAFh
lahf
wait
mov edx, 84874BB6h
inc ebx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x114e4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x15c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xe4	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x108f4	0x11000	False	0.360337201287	data	5.30760673426	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0x118c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x15c8	0x2000	False	0.137573242188	data	1.7754215961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x153e0	0x1e8	data		
RT_ICON	0x14d18	0x6c8	data		
RT_ICON	0x14390	0x988	data		
RT_GROUP_ICON	0x14360	0x30	data		
RT_VERSION	0x14150	0x210	data	Greek	Greece

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaCastObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarDup, __vbaVarLateMemCallLd, __vbaFpI4, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0408 0x04b0
InternalName	sweepers
FileVersion	2.00
CompanyName	Gallup
ProductName	Gallup
ProductVersion	2.00
OriginalFilename	sweepers.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Greek	Greece	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:58:17.964037895 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.098231077 CET	443	49748	192.185.152.65	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:58:18.098367929 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.115515947 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.249711037 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.254128933 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.254153013 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.254163027 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.254322052 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.254345894 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.336226940 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.471143961 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.471311092 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.487610102 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.627404928 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627434015 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627445936 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627459049 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627475023 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627494097 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627511024 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627526045 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627542019 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627557993 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.627580881 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.627635002 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.761832952 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761864901 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761878014 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761889935 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761900902 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761914968 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761931896 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761948109 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761964083 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761981964 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.761998892 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762011051 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762022972 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762038946 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762053967 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.762054920 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762070894 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762087107 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762100935 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762116909 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762124062 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.762137890 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.762164116 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.762191057 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896260023 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896287918 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896301031 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896316051 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896336079 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896353006 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896369934 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896387100 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896399021 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896403074 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896419048 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896435976 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896440983 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896451950 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896471977 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896473885 CET	49748	443	192.168.2.4	192.185.152.65

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:58:18.896488905 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896491051 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896506071 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896521091 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896528959 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896537066 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896553040 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896559000 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896569014 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896579027 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896584988 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896605968 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896606922 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896634102 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896640062 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896652937 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896668911 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896671057 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896683931 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896699905 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896707058 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896718025 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896734953 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896742105 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896749973 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896763086 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896766901 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896783113 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896789074 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896797895 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896814108 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896821022 CET	49748	443	192.168.2.4	192.185.152.65
Nov 20, 2020 10:58:18.896830082 CET	443	49748	192.185.152.65	192.168.2.4
Nov 20, 2020 10:58:18.896847963 CET	443	49748	192.185.152.65	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:57:44.504728079 CET	64549	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:44.531829119 CET	53	64549	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:45.892416954 CET	63153	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:45.919528961 CET	53	63153	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:50.394385099 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:50.421511889 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:51.438606977 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:51.465647936 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:52.895874977 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:52.922995090 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:54.024133921 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:54.051191092 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:55.123883009 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:55.151484966 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:56.756340981 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:56.794018030 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 10:57:58.006989002 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:57:58.034130096 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:00.145034075 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:00.172065973 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:01.189306021 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:01.216273069 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:02.337378025 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:02.372955084 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:03.486059904 CET	61721	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 10:58:03.513978958 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:04.649158955 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:04.676244974 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:13.701463938 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:13.728507996 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:17.910629034 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:17.946242094 CET	53	52337	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:37.646971941 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:37.685893059 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:38.271760941 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:38.307430983 CET	53	49612	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:38.732089043 CET	49285	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:38.767661095 CET	53	49285	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:39.490035057 CET	50601	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:39.525820017 CET	53	50601	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:39.994446039 CET	60875	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:40.047394037 CET	53	60875	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:40.602123976 CET	56448	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:40.637559891 CET	53	56448	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:42.347006083 CET	59172	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:42.382642984 CET	53	59172	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:45.332072973 CET	62420	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:45.367695093 CET	53	62420	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:45.938966990 CET	60579	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:45.985002995 CET	53	60579	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:46.336373091 CET	50183	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:46.373931885 CET	53	50183	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:46.387773991 CET	61531	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:46.438936949 CET	53	61531	8.8.8.8	192.168.2.4
Nov 20, 2020 10:58:53.257333994 CET	49228	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:58:53.294634104 CET	53	49228	8.8.8.8	192.168.2.4
Nov 20, 2020 10:59:16.030581951 CET	59794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:59:16.171674967 CET	53	59794	8.8.8.8	192.168.2.4
Nov 20, 2020 10:59:23.233150959 CET	55916	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:59:23.260363102 CET	53	55916	8.8.8.8	192.168.2.4
Nov 20, 2020 10:59:24.740112066 CET	52752	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:59:24.775619030 CET	53	52752	8.8.8.8	192.168.2.4
Nov 20, 2020 10:59:36.980271101 CET	60542	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:59:37.143199921 CET	53	60542	8.8.8.8	192.168.2.4
Nov 20, 2020 10:59:57.368199110 CET	60689	53	192.168.2.4	8.8.8.8
Nov 20, 2020 10:59:57.535033941 CET	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 10:58:17.910629034 CET	192.168.2.4	8.8.8.8	0x1d6a	Standard query (0)	pilatescol lective.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:16.030581951 CET	192.168.2.4	8.8.8.8	0x8d36	Standard query (0)	www.yourdf wliving.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:36.980271101 CET	192.168.2.4	8.8.8.8	0x1d46	Standard query (0)	www.goldkiili.com	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:57.368199110 CET	192.168.2.4	8.8.8.8	0x4018	Standard query (0)	www.remote reg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 10:58:17.946242094 CET	8.8.8.8	192.168.2.4	0x1d6a	No error (0)	pilatescol lective.com		192.185.152.65	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:16.171674967 CET	8.8.8.8	192.168.2.4	0x8d36	No error (0)	www.yourdf wliving.com		64.98.145.30	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:37.143199921 CET	8.8.8.8	192.168.2.4	0x1d46	Name error (3)	www.goldki ili.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 10:59:57.535033941 CET	8.8.8.8	192.168.2.4	0x4018	No error (0)	www.remotereg.com		45.79.19.196	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:57.535033941 CET	8.8.8.8	192.168.2.4	0x4018	No error (0)	www.remotereg.com		45.33.23.183	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:57.535033941 CET	8.8.8.8	192.168.2.4	0x4018	No error (0)	www.remotereg.com		198.58.118.167	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:57.535033941 CET	8.8.8.8	192.168.2.4	0x4018	No error (0)	www.remotereg.com		96.126.123.244	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:57.535033941 CET	8.8.8.8	192.168.2.4	0x4018	No error (0)	www.remotereg.com		45.56.79.23	A (IP address)	IN (0x0001)
Nov 20, 2020 10:59:57.535033941 CET	8.8.8.8	192.168.2.4	0x4018	No error (0)	www.remotereg.com		45.33.2.79	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.yourdfwliving.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49765	64.98.145.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 10:59:16.288027048 CET	5777	OUT	GET /ca5e/?9rmT0Zz8=33d4ALcEm9QS3ETZfm99n5/91vkYSjLj82bPV1gW1bkPYk/ky+qZQnI1oXWMSZEPGOwK&rZ=Xn8pd6vp HTTP/1.1 Host: www.yourdfwliving.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 10:59:16.403343916 CET	5778	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Status: 200 OK X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff ETag: W/"afd398a585c4066e64ccec8c4d526b3c" Cache-Control: max-age=0, private, must-revalidate X-Request-Id: ff03b95c-7114-4942-8680-826c1f30776e X-Runtime: 0.006637 X-Powered-By: Phusion Passenger 4.0.53 Date: Fri, 20 Nov 2020 10:10:38 GMT Server: nginx/1.6.2 + Phusion Passenger 4.0.53 P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT" Data Raw: 31 37 33 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 27 20 68 74 74 70 2d 65 71 75 69 76 3d 27 43 6f 6e 74 65 6e 74 2d 54 79 70 65 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 33 43 62 61 56 76 77 2d 49 37 4d 6c 72 6d 6d 6d 48 7a 30 62 66 62 6b 6f 37 6f 4d 43 57 31 6d 6e 32 75 36 35 75 57 73 57 57 42 38 27 20 6e 61 6d 65 3d 27 67 6f 6f 67 6c 65 2d 73 69 74 65 2d 76 65 72 69 66 69 63 61 74 69 6f 6e 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 27 20 6e 61 6d 65 3d 27 76 69 65 77 70 6f 72 74 27 3e 0a 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 27 74 65 6c 65 70 68 6f 6e 65 3d 6e 6f 27 20 6e 61 6d 65 3d 27 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 27 3e 0a 3c 74 69 74 6c 65 3e 79 6f 75 72 64 66 77 6c 69 76 69 6e 67 2e 63 6f 6d 20 69 73 20 63 6f 6d 69 6e 67 20 73 6f 6f 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4f 70 65 6e 2b 53 61 6e 73 3a 33 30 30 2c 34 30 30 2c 36 30 30 2c 37 30 30 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 20 68 72 65 66 3d 22 2f 61 73 73 65 74 73 2f 61 70 70 6c 69 63 61 74 69 6f 6e 2d 32 66 37 65 37 66 33 30 64 38 31 32 64 30 66 33 39 35 30 39 31 38 63 37 35 36 32 64 66 37 65 36 38 65 65 65 65 62 64 38 36 34 39 62 64 65 61 32 62 63 33 38 34 34 65 62 30 37 66 63 38 32 36 39 2e 63 73 73 22 20 2f 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 65 61 64 65 72 3e 0a 3c 61 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 6f 76 65 72 2e 63 6f 6d 2f 3f 73 6f 75 72 63 65 3d 70 61 72 6b 65 64 22 3e 3c 69 6d 67 20 77 69 64 74 68 3d 22 31 30 32 22 20 68 65 69 67 68 74 3d 22 33 30 22 20 73 72 63 3d 22 2f 61 73 73 65 74 73 2f 68 76 5f 6c 6f Data Ascii: 173d<!DOCTYPE html><html><head><meta content='text/html; charset=UTF-8' http-equiv='Content-Type'><meta content='3CbaVvw-I7MlrmmmHz0bfbko7oMCW1mn2u65uWsWWB8' name='google-site-verification'><meta content='width=device-width, initial-scale=1.0' name='viewport'><meta content='telephone=no' name='format-detection'><title>yourdfwliving.com is coming soon</title><link rel="stylesheet" media="screen" href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700" /><link rel="stylesheet" media="all" href="/assets/application-2f7e7f30d812d0f3950918c7562df7e68eeeebd8649bdea2bc3844eb07fc8269.css" /></head><body><header><a rel="nofollow" href="https://www.hover.com/?source=parked"><img width="102" height="30" src="/assets/hv_lo

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 10:58:18.254163027 CET	192.185.152.65	443	192.168.2.4	49748	CN=www.pilatescollective.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Nov 06 01:22:43 CET 2020	Thu Feb 04 01:22:43 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

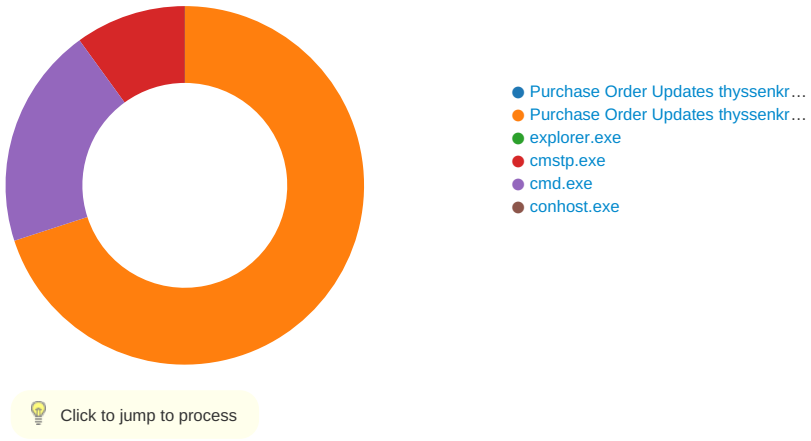
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE7
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE7
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE7
GetMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE7

Statistics

Behavior



System Behavior

Analysis Process: Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe PID: 6304 Parent PID: 5868

General

Start time:	10:57:48
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	6008CD180E677BE4846D5F8ABFA6B983
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe PID: 6780 Parent PID: 6304

General

Start time:	10:58:03
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	6008CD180E677BE4846D5F8ABFA6B983
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.757374606.00000000000A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.757374606.00000000000A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.757374606.00000000000A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.761692759.000000001E150000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.761692759.000000001E150000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.761692759.000000001E150000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

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	564F17	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564F17	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564F17	InternetOpenUrlA
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	564F17	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564F17	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564F17	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E37	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6780

General

Start time:	10:58:19
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmstp.exe PID: 6004 Parent PID: 3424

General

Start time:	10:58:34
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x830000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.921168798.0000000002E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.921168798.0000000002E40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.921168798.0000000002E40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.920987753.0000000002960000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.920987753.0000000002960000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.920987753.0000000002960000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.921197000.0000000002E70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.921197000.0000000002E70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.921197000.0000000002E70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000006.00000002.922109924.0000000004FFF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000006.00000002.921254049.0000000002EBE000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2979E37	NtReadFile

Analysis Process: cmd.exe PID: 2108 Parent PID: 6004

General

Start time:	10:58:39
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 2860 Parent PID: 2108

General

Start time:	10:58:39
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis