



ID: 356551
Sample Name: PO Contract - SCPL0882021 & sales contract ZD.1.19022021_PDF.exe
Cookbook: default.jbs
Time: 10:00:05
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Networking: 5
System Summary: 5
Data Obfuscation: 6
Malware Analysis System Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 14
Public 14
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 17
ASN 17
JA3 Fingerprints 17
Dropped Files 18
Created / dropped Files 18
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18

Entrypoint Preview 19
Data Directories 20
Sections 20
Resources 21
Imports 21
Version Infos 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 22
DNS Queries 24
DNS Answers 24
SMTP Packets 24
Code Manipulations 24
Statistics 24
System Behavior 24
Analysis Process: PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe PID: 6968 Parent PID: 5868 24
General 24
File Activities 25
File Created 25
File Read 25
Disassembly 26
Code Analysis 26

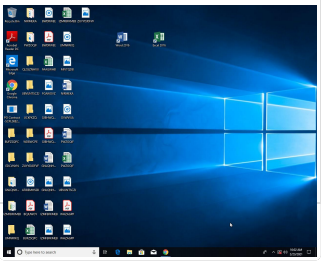
Analysis Report PO Contract -SCPL0882021 & sales con…

Overview

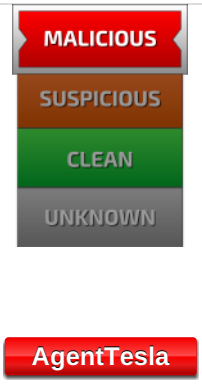
General Information

Sample Name:	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe
Analysis ID:	356551
MD5:	1aee76519a71de..
SHA1:	7a0138e465d7dd..
SHA256:	95d7e599e9a764..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



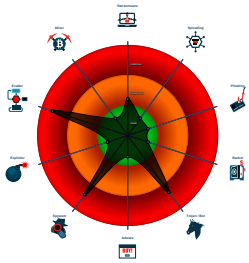
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe (PID: 6968 cmdline: 'C:\Users\user\Desktop\PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe' MD5: 1AEE76519A71DE3F3F4E7485C2FCC9CB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "bWUSNsqFz",
  "URL: ": "http://hWJRHFah1ZO6.com",
  "To: ": "fikriye@turuncoglu.com",
  "ByHost: ": "smtp.yandex.com:587",
  "Password: ": "WYVxdnuS0dPp19",
  "From: ": "fikriye@turuncoglu.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.912083568.000000000285 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.912083568.000000000285 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000000.00000002.924538970.0000000008A3 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.913283629.0000000003AD 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: PO Contract -SCPL0882021 & s ales contract ZD.1.19022021_PDF.exe PID: 6968	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright null 2021

Source	Rule	Description	Author	Strings
Click to see the 2 entries				

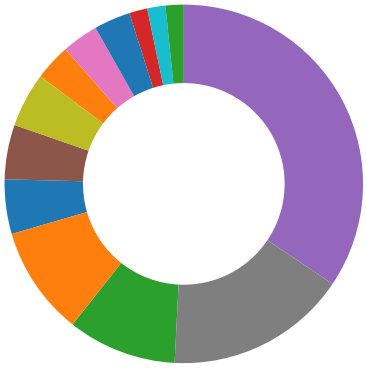
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO Contract -SCPL0882021 & sales contract ZD.1 .19022021_PDF.exe.3b21d90.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO Contract -SCPL0882021 & sales contract ZD.1 .19022021_PDF.exe.8a30000.11.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO Contract -SCPL0882021 & sales contract ZD.1 .19022021_PDF.exe.8a30000.11.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO Contract -SCPL0882021 & sales contract ZD.1 .19022021_PDF.exe.3b21d90.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO Contract -SCPL0882021 & sales contract ZD.1 .19022021_PDF.exe.288692c.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:



Uses 32bit PE files

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

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:



.NET source code contains potential unpacker

Malware Analysis System Evasion:



Yara detected AntiVM_3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Stealing of Sensitive Information:



Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

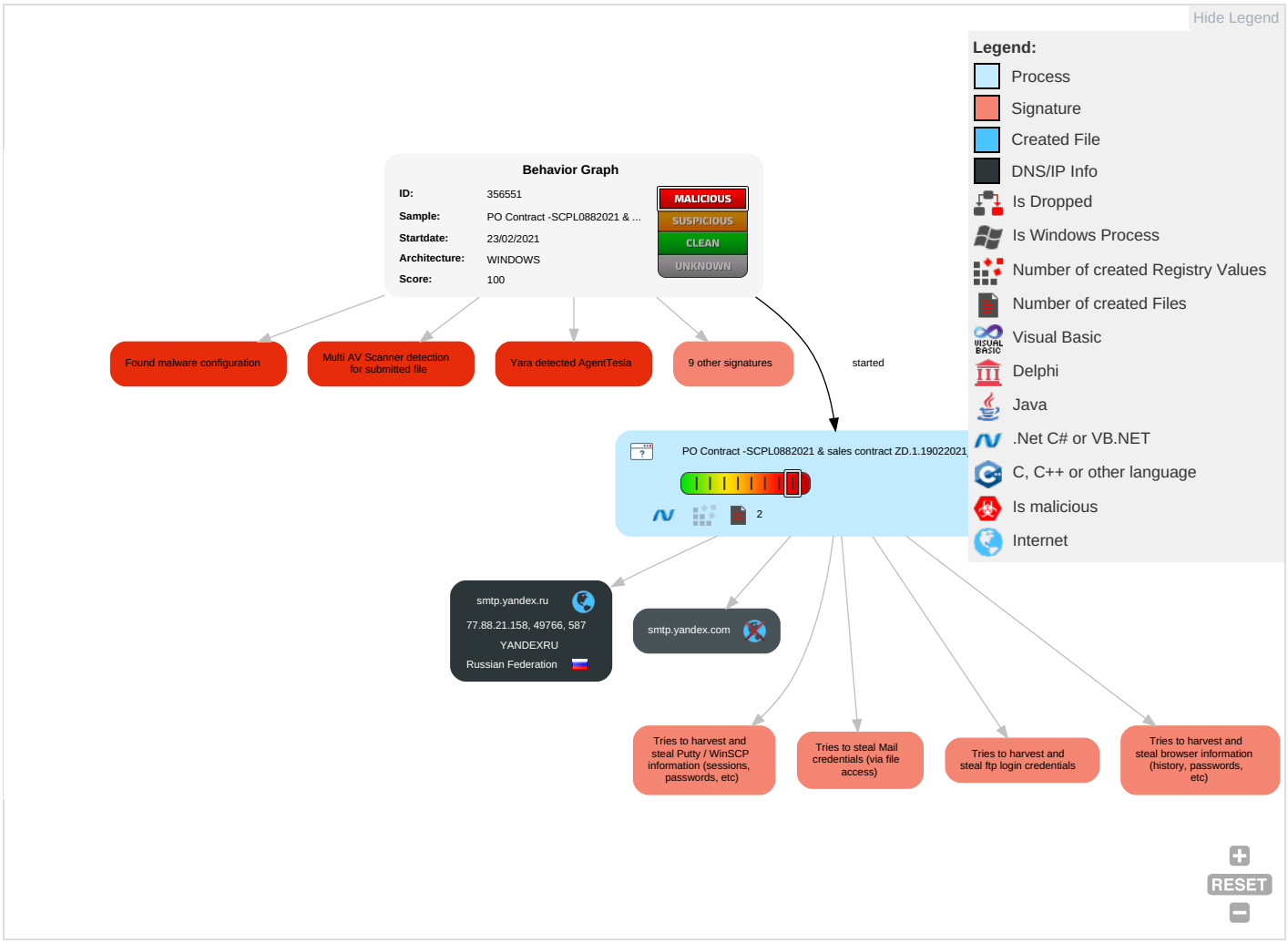


Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 3	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2 1	NTDS	Process Discovery 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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
PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://crls.yandex	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	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.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://yandex.crl.certum.	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.fonts.como	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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://repository.cert	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.fontbureau.comdiaa;	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://hWJRHFah1ZO6.com	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://NfuOAc.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd6	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlr	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hWJRHFah1ZO6.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9120835 68.0000000002851000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://www.fontbureau.com/designers/?	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high

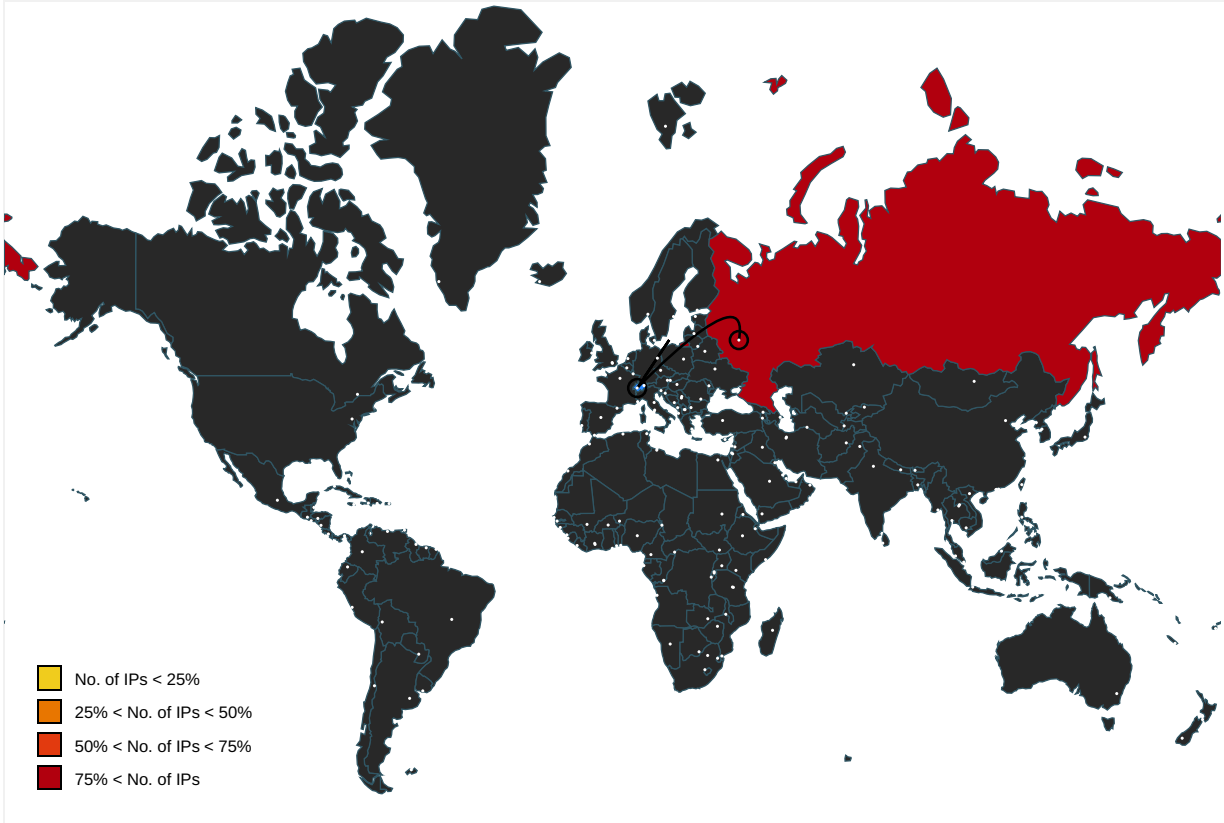
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://yandex.crl.certum.pl/ycasha2.crl0q	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high
http://www.tiro.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://www.goodfont.co.kr	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crls.yandex	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9120835 68.0000000002851000.00000004.0 0000001.sdmp	false		high
http://www.sajatypeworks.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp, PO Contract -SCP L0882021 & sales contract ZD.1 .19022021_PDF.exe, 00000000.00 000003.645752461.0000000005903 000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comgrita	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.915436584.0000000005900000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.924040060.00000000087BF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.crl.certum.	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.924040060.00000000087BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.como	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.646314068.000000000591B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.cert	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.924040060.00000000087BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.come	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.645752461.0000000005903000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.924538970.0000000008A30000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.924040060.00000000087BF000.00000004.00000001.sdmp	false		high
http://repository.certum.pl/ycasha2.cer0	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.924040060.00000000087BF000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.917008175.0000000006B12000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://DynDns.comDynDNS	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9120835 68.0000000002851000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high
http://www.sajatypeworks.comt	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.6457524 61.0000000005903000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comdiaa;	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9154365 84.0000000005900000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	low
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9120835 68.0000000002851000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high
http://https://www.certum.pl/CPS0	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high
http://en.w	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.6462415 25.0000000005905000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.yandex.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9125806 09.0000000002B81000.00000004.0 0000001.sdmp	false		high
http://NfuOAc.com	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9120835 68.0000000002851000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.ocsp-responder.com03	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.6486862 18.0000000005906000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://www.founder.com.cn/cn	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.6486862 18.0000000005906000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0-	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high
http://www.founder.com.cn/cnd6	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.6480478 54.000000000590E000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlr	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000003.6510390 87.000000000593D000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9154365 84.0000000005900000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9170081 75.0000000006B12000.00000004.0 0000001.sdmp	false		high
http://crl.certum.pl/ca.crl0h	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe, 00000000.00000002.9240400 60.00000000087BF000.00000004.0 0000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	unknown	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356551
Start date:	23.02.2021
Start time:	10:00:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/0@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.11.168.160, 13.107.3.254, 13.107.246.254, 13.64.90.137, 104.43.193.48, 92.122.145.220, 13.88.21.125, 40.88.32.150, 52.147.198.201, 51.104.139.180, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356551/sample/PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe

Simulations

Behavior and APIs

Time	Type	Description
10:01:00	API Interceptor	767x Sleep call for process: PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	pass.exe	Get hash	malicious	Browse	
	nXKdiUgIYy.exe	Get hash	malicious	Browse	
	x4cXV3784J.exe	Get hash	malicious	Browse	
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	
	emI0MqOvFw.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZnsXrCAriL.exe	Get hash	malicious	Browse	
	zyp9gbDQHw.exe	Get hash	malicious	Browse	
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	
	MI3eskSuv2.exe	Get hash	malicious	Browse	
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	
	feb 16 processed.xlsx	Get hash	malicious	Browse	
	IMG_Catalogue Document.exe	Get hash	malicious	Browse	
	PO#THE786YT_pdf.exe	Get hash	malicious	Browse	
	BL_No#ONEYJKTAC6384600.exe	Get hash	malicious	Browse	
	DHL Delivery Documents.exe	Get hash	malicious	Browse	
	Scan copy.exe	Get hash	malicious	Browse	
	jmsg.exe	Get hash	malicious	Browse	
	DOC11022012.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158
	zyp9gbDQHw.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	MI3eskSuv2.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	feb 16 processed.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	IMG_Catalogue Document.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#THE786YT_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	BL_No#ONEYJKTAC6384600.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Delivery Documents.exe	Get hash	malicious	Browse	• 77.88.21.158
	Scan copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	jmsg.exe	Get hash	malicious	Browse	• 77.88.21.158
	DOC11022012.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	pass.exe	Get hash	malicious	Browse	• 77.88.21.158
	nXKdiUgIYy.exe	Get hash	malicious	Browse	• 77.88.21.158
	x4cXV3784J.exe	Get hash	malicious	Browse	• 77.88.21.158
	Request For Quotation #D22022021_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ_PDRVK2200248_00667_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	emI0MqOvFw.exe	Get hash	malicious	Browse	• 77.88.21.158
	ZnsXrCAriL.exe	Get hash	malicious	Browse	• 77.88.21.158
	zyp9gbDQHw.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Shipment Notification.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	MI3eskSuv2.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	NUANG KONG-ON2343020-146377_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	feb 16 processed.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	IMG_Catalogue Document.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#THE786YT_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	BL_No#ONEYJKTAC6384600.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL Delivery Documents.exe	Get hash	malicious	Browse	• 77.88.21.158
	Scan copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	jmsg.exe	Get hash	malicious	Browse	• 77.88.21.158
	DOC11022012.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

Copyright null 2021

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.499133080349246
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:	PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe
File size:	545280
MD5:	1aee76519a71de3f3f4e7485c2fcc9cb
SHA1:	7a0138e465d7dd20a726f3ccebf811b059355dd4
SHA256:	95d7e599e9a76497dd73084440554dfcf4a94974d49e88 43f23611d4bce5d12
SHA512:	8f039b136c2c49adee9aaf92b881702a81dfba08a5ae472 26d5b41c267fc475471b4d7ecf2b3c8ac06234f8a97c738 ac026d2f298e275c1f759609b578a7a4b3
SSDEEP:	12288:MUnrX5P0QUsmn1vCn3AhvNKwBEw88+dtEYb DYBNeLrdqWrlFCP4JM:brX5PsseEn0vmwSXYBNe0W xYcM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o4`.....P..<.....Z... ...`....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x485a9e
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:	0x60346F84 [Tue Feb 23 02:59:16 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

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

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x83aa4	0x83c00	False	0.779986213235	data	7.51402994346	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x1018	0x1200	False	0.360243055556	data	4.71646584206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x86090	0x364	data		
RT_MANIFEST	0x86404	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

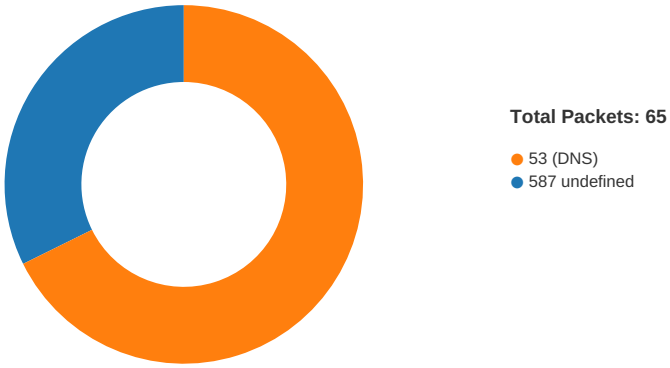
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:02:42.198137045 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.278058052 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.278263092 CET	49766	587	192.168.2.4	77.88.21.158

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:02:42.495795012 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.496234894 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.576133966 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.576175928 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.577894926 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.657800913 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.703923941 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.756781101 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.837865114 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.837910891 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.837932110 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.837953091 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:42.838053942 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.838130951 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.895100117 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:42.975493908 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.016398907 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.314435005 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.394462109 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.396380901 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.476207972 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.477214098 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.572707891 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.573838949 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.662101984 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.662761927 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.750448942 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.751246929 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.831873894 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.834738016 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.835112095 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.835944891 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.836241007 CET	49766	587	192.168.2.4	77.88.21.158
Feb 23, 2021 10:02:43.914947987 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:43.916039944 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:44.468914032 CET	587	49766	77.88.21.158	192.168.2.4
Feb 23, 2021 10:02:44.516482115 CET	49766	587	192.168.2.4	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:00:43.904242992 CET	53723	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:43.953201056 CET	53	53723	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:44.008800983 CET	64646	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:44.057655096 CET	53	64646	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:44.253242970 CET	65298	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:44.301928997 CET	53	65298	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:44.391328096 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:44.440063953 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:46.598134041 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:46.649734020 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:47.582580090 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:47.633573055 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:48.228200912 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:48.286237955 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:49.299523115 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:49.351027966 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:50.944117069 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:50.992784023 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:52.594340086 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:52.655049086 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:54.342374086 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:54.391372919 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:55.159972906 CET	55854	53	192.168.2.4	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:00:55.211529016 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:56.114887953 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:56.174813986 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:57.107119083 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:57.156094074 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:58.200087070 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:58.248769999 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 10:00:59.456084967 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:00:59.515988111 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:00.498574018 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:00.550203085 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:01.660548925 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:01.709533930 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:02.429672956 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:02.478437901 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:03.334944963 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:03.387681007 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:04.456754923 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:04.505563974 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:05.337758064 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:05.387083054 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:07.280673027 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:07.332103014 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:08.597980976 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:08.655253887 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:20.470321894 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:20.518882990 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:36.786833048 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:36.853599072 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:37.528295040 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:37.602746010 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:38.140194893 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:38.203047037 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:38.570153952 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:38.638699055 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:38.725440025 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:38.783823967 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:39.243807077 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:39.305532932 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:39.881556988 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:39.905564070 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:39.941510916 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:39.964632034 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:40.666313887 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:40.724735022 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:42.018938065 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:42.076061964 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:43.104039907 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:43.160797119 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:43.684237003 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:43.733505011 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:54.736334085 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:54.784964085 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:55.000256062 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:55.072727919 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 10:01:57.758444071 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:01:57.817082882 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 10:02:31.309809923 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:02:31.358388901 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 10:02:33.507487059 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:02:33.572231054 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 10:02:41.925867081 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:02:41.985615015 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 10:02:42.019001007 CET	60542	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:02:42.075989008 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:02:41.925867081 CET	192.168.2.4	8.8.8.8	0x13a7	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:02:42.019001007 CET	192.168.2.4	8.8.8.8	0x411	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:02:41.985615015 CET	8.8.8.8	192.168.2.4	0x13a7	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:02:41.985615015 CET	8.8.8.8	192.168.2.4	0x13a7	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Feb 23, 2021 10:02:42.075989008 CET	8.8.8.8	192.168.2.4	0x411	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:02:42.075989008 CET	8.8.8.8	192.168.2.4	0x411	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 10:02:42.495795012 CET	587	49766	77.88.21.158	192.168.2.4	220 vla4-d1b041059520.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Feb 23, 2021 10:02:42.496234894 CET	49766	587	192.168.2.4	77.88.21.158	EHLO 928100
Feb 23, 2021 10:02:42.576175928 CET	587	49766	77.88.21.158	192.168.2.4	250-vla4-d1b041059520.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Feb 23, 2021 10:02:42.577894926 CET	49766	587	192.168.2.4	77.88.21.158	STARTTLS
Feb 23, 2021 10:02:42.657800913 CET	587	49766	77.88.21.158	192.168.2.4	220 Go ahead

Code Manipulations

Statistics

System Behavior

Analysis Process: PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe PID: 6968 Parent PID: 5868

General

Start time:	10:00:52
Start date:	23/02/2021

Copyright null 2021

Path:	C:\Users\user\Desktop\PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO Contract -SCPL0882021 & sales contract ZD.1.19022021_PDF.exe'
Imagebase:	0x3e0000
File size:	545280 bytes
MD5 hash:	1AEE76519A71DE3F3F4E7485C2FCC9CB
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: 00000000.00000002.912083568.0000000002851000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.912083568.0000000002851000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.924538970.0000000008A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.913283629.0000000003AD3000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D19CF06	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	6D19CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D175705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D17CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\48542f46-1c69-43e1-b4fa-88e24b9018f4	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFE1B4F	ReadFile

Disassembly

Code Analysis