ID: 532730
Sample Name: new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
Cookbook: default.jbs
Time: 16:48:50
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Boot Survival: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection 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 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 14
Imports 14
Version Infos 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
SMTP Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15

Analysis Process: new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe PID: 4252 Parent PID: 6088 15
General 15
File Activities 16
File Created 16
File Deleted 16
File Written 16
File Read 16
Analysis Process: schtasks.exe PID: 2964 Parent PID: 4252 16
General 16
File Activities 16
File Read 16
Analysis Process: conhost.exe PID: 3336 Parent PID: 2964 16
General 16
Analysis Process: new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe PID: 4792 Parent PID: 4252 17
General 17
File Activities 17
File Created 17
File Read 17
Disassembly 17
Code Analysis 17

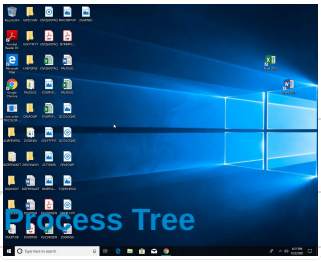
Windows Analysis Report new order TRICOLOR-6.45 TR…

Overview

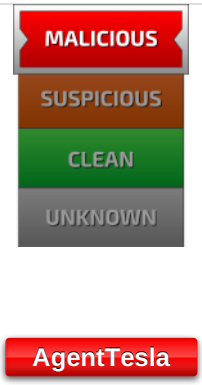
General Information

Sample Name:	new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
Analysis ID:	532730
MD5:	66cbe976594f666.
SHA1:	944c8819e41ad5..
SHA256:	460eb466736267..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection

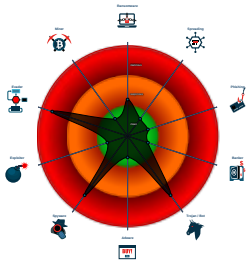


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…

Classification



- **System is w10x64**
- new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe (PID: 4252 cmdline: "C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe" MD5: 66CBE976594F666D5440264A4084B21F)
  - schtasks.exe (PID: 2964 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\aUkURZiJ" /XML "C:\Users\user\AppData\Local\Temp\tmp8923.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe (PID: 4792 cmdline: {path} MD5: 66CBE976594F666D5440264A4084B21F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "marketing@kyowasecurity.com.sg",
  "Password": "avKw1$991",
  "Host": "mail.kyowasecurity.com.sg"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.282084634.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.282084634.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.283151659.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.283151659.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.287974260.000000000276 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.3922928.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

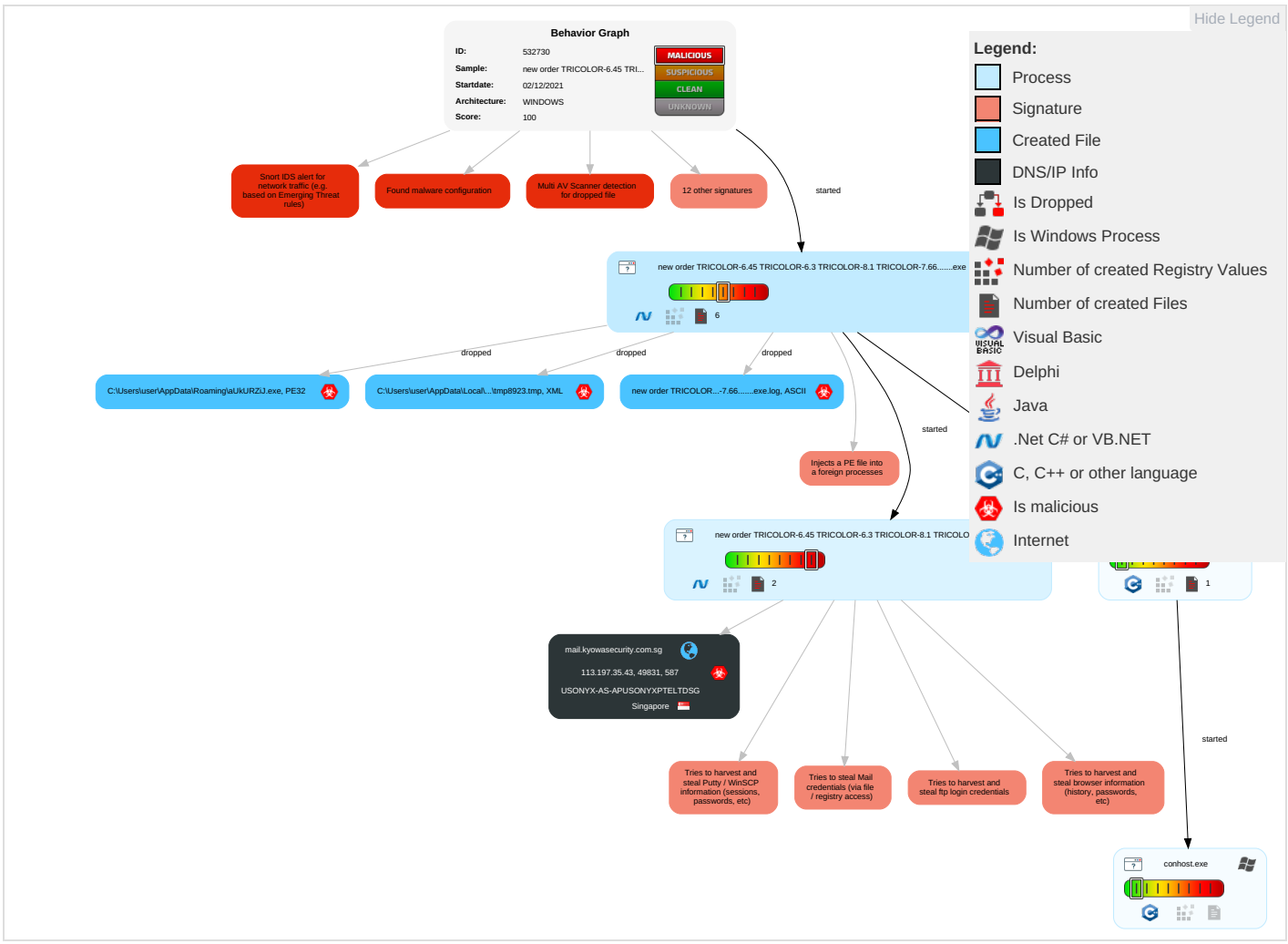
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

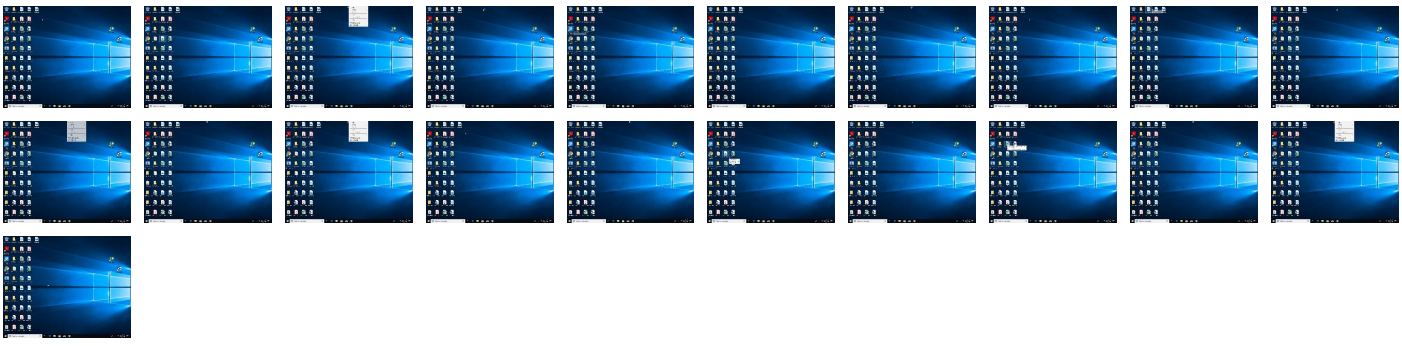
Behavior Graph



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
new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\aUkURZiJ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\aUkURZiJ.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.urwpp.demM	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ys;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0y	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTFks	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed3sm	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.tiro.comD	0%	Avira URL Cloud	safe	
http://www.urwpp.de.T	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	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.jiyu-kobo.co.jp/ks	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ch	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comttv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	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://www.fontbureau.comtuta	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/OsI	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiva	0%	URL Reputation	safe	
http://mail.kyowasecurity.com.sg	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	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://KpGsSw.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deF	0%	URL Reputation	safe	
http://www.fontbureau.comVsF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comzana	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	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/ms	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comdrs	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/OsI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/VsF	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/3sm	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.kyowasecurity.com.sg	113.197.35.43	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
113.197.35.43	mail.kyowasecurity.com.sg	Singapore		38532	USONYX-AS-APUSONYXPTELTDSG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532730
Start date:	02.12.2021
Start time:	16:48:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....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:	21
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@6/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.3%) • Quality average: 34.4% • Quality standard deviation: 37.2%
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

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:49:58	API Interceptor	614x Sleep call for process: new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
113.197.35.43	AWB#8001187 SHIPPING DOCUMENTS PL+BL+CI.exe	Get hash	malicious	Browse	
	SHIPMENT DOCUMENTS FOR 912 INVOICE - PL+ CI+BL+ORIGINCERT.exe	Get hash	malicious	Browse	
	urgent request fro quotation CONO GROUP LLC DK9837 46GT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.kyowasecurity.com.sg	AWB#8001187 SHIPPING DOCUMENTS PL+BL+CI.exe	Get hash	malicious	Browse	• 113.197.35.43
	SHIPMENT DOCUMENTS FOR 912 INVOICE - PL+ CI+BL+ORIGINCERT.exe	Get hash	malicious	Browse	• 113.197.35.43
	urgent request fro quotation CONO GROUP LLC DK9837 46GT.exe	Get hash	malicious	Browse	• 113.197.35.43

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
USONYX-AS-APUSONYXPTELTDSG	(SA213-317L)_INHA_20211122.exe	Get hash	malicious	Browse	• 103.7.9.22
	zhaP868fw5	Get hash	malicious	Browse	• 43.229.194.252
	lDawzTbABc	Get hash	malicious	Browse	• 43.229.194.215
	juxSAmZoqx	Get hash	malicious	Browse	• 103.36.93.250
	Ynffczq7m4	Get hash	malicious	Browse	• 43.229.194.223
	RFQ_LISTaugust2315.exe	Get hash	malicious	Browse	• 103.7.8.203
	loligang.x86	Get hash	malicious	Browse	• 43.229.193.74
	TFG18FA4eD	Get hash	malicious	Browse	• 43.229.194.255
	Order 824126.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 161488.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 824126.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 161488.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 46975986.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	PO 97179275.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 46975986.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 2522592.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	PO 97179275.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	Order 2522592.xlsb	Get hash	malicious	Browse	• 116.12.51.202
	AWB#8001187 SHIPPING DOCUMENTS PL+BL+CI.exe	Get hash	malicious	Browse	• 113.197.35.43
	SHIPMENT DOCUMENTS FOR 912 INVOICE - PL+ CI+BL+ORIGINCERT.exe	Get hash	malicious	Browse	• 113.197.35.43

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe.log	
Process:	C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp8923.tmp	
Process:	C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.172468542885359
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBeNtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3e
MD5:	6D873C913C6BA247539E8D716FDF3A91
SHA1:	9CDD0F46D6C29970CE6E9D2B60978BD2A4B5419F
SHA-256:	098DBD4D3FA82AEAD5B22CA909E2FF9281FC1970123DF7952AE43577FB556BC0
SHA-512:	1683A3EF8053E0E2A8ECE7349CA1E2104164E5D870A9A748DCCD4856CF073CF5B3C088A29D44BD8D354914BC36578F4037B64028396CEB59D0869677DB2061F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\aUkURZiJ.exe	
Process:	C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	562688
Entropy (8bit):	7.620214969982571
Encrypted:	false
SSDEEP:	12288:j2KwyZTuK+jJ8CXnZQ6VlgyoRPWHN3dvos/:jhyVpQ6VG+7v
MD5:	66CBE976594F666D5440264A4084B21F
SHA1:	944C8819E41AD59333527141A7FD5180253969E1
SHA-256:	460EB4667362671BE2BE1E94AFE56E73331C3A3CD58B028E49EC135FEC8888A9
SHA-512:	1EBB035FD7CEAB82F4EE270E66B097958E8B57805897DCAFC4736E82E64961EC5DF61AF8A0EC78D9D119D2EC235D955559CFE360587E46915AA9C5450C93DAE
Malicious:	**true**

C:\Users\user\AppData\Roaming\aUkURZiJ.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....k.....P..... .....@.. ..@.....I...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....X.....`%.....0.....*....0..... $.cG ..xa%..^E.....+.(....(..... .?.Z .P4Ka+..... .... ..xa%..^E. .....,...+*(.....o..... .,).Z .C6.a+... ..kZ ....a+.*.....?@.....0..*.....(.....(!.....("......(#.....($....*...0..D..... .'.. b.[.a%..^E....!.....+..(....o....(%.... }$D.Z .i oa+..*.0..: .....(&... ..Y. .i.a%..^E.....+... .J.lZ D.<a+.*...0..w...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.620214969982571
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:	new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
File size:	562688
MD5:	66cbe976594f666d5440264a4084b21f
SHA1:	944c8819e41ad59333527141a7fd5180253969e1
SHA256:	460eb4667362671be2be1e94afe56e73331c3a3cd58b028e49ec135fec8888a9
SHA512:	1ebb035fd7ceab82f4ee270e66b097958e8b57805897dcafc4736e82e64961ec5df61af8a0ec78d9d119d2ec235d955559cfe360587e46915aa9c5450c93da1e
SSDEEP:	12288:j2KwyZTuK+jJ8CXnZQ6VlgyoRPWHN3dvos/:jhyVpQ6VG+7v
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....k.....P..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48aabe
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:	0xAC6B97B1 [Wed Aug 31 16:45:37 2061 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

General

Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x88ac4	0x88c00	False	0.813471206581	data	7.63105429026	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x5a0	0x600	False	0.421223958333	data	4.0719135687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-16:51:59.303417	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49831	587	192.168.2.5	113.197.35.43

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 16:51:53.977710962 CET	192.168.2.5	8.8.8.8	0x6725	Standard query (0)	mail.kyowasecurity.com.sg	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 16:51:54.132426977 CET	8.8.8.8	192.168.2.5	0x6725	No error (0)	mail.kyowasecurity.com.sg		113.197.35.43	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 16:51:57.680073023 CET	587	49831	113.197.35.43	192.168.2.5	220 spinworksmail2020.spinworks.com.sg ESMTP Postfix
Dec 2, 2021 16:51:57.680427074 CET	49831	587	192.168.2.5	113.197.35.43	EHLO 128757

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 16:51:57.948971033 CET	587	49831	113.197.35.43	192.168.2.5	250-spinworksmail2020.spinworks.com.sg 250-PIPELINING 250-SIZE 30720000 250-ETRN 250-STARTTLS 250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Dec 2, 2021 16:51:57.949990034 CET	49831	587	192.168.2.5	113.197.35.43	AUTH login bWFya2V0aW5nQGt5b3dhc2VjdXJpdHkuY29tLnNn
Dec 2, 2021 16:51:58.218070984 CET	587	49831	113.197.35.43	192.168.2.5	334 UGFzc3dvcmQ6
Dec 2, 2021 16:51:58.487137079 CET	587	49831	113.197.35.43	192.168.2.5	235 2.7.0 Authentication successful
Dec 2, 2021 16:51:58.487844944 CET	49831	587	192.168.2.5	113.197.35.43	MAIL FROM:<marketing@kyowasecurity.com.sg>
Dec 2, 2021 16:51:58.756607056 CET	587	49831	113.197.35.43	192.168.2.5	250 2.1.0 Ok
Dec 2, 2021 16:51:58.756807089 CET	49831	587	192.168.2.5	113.197.35.43	RCPT TO:<marketing@kyowasecurity.com.sg>
Dec 2, 2021 16:51:59.032618999 CET	587	49831	113.197.35.43	192.168.2.5	250 2.1.5 Ok
Dec 2, 2021 16:51:59.032835960 CET	49831	587	192.168.2.5	113.197.35.43	DATA
Dec 2, 2021 16:51:59.302530050 CET	587	49831	113.197.35.43	192.168.2.5	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 16:51:59.304236889 CET	49831	587	192.168.2.5	113.197.35.43	.
Dec 2, 2021 16:51:59.805361986 CET	587	49831	113.197.35.43	192.168.2.5	250 2.0.0 Ok: queued as CFC00DFA092

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe PID: 4252 Parent PID: 6088

General

Start time:	16:49:48
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe"
Imagebase:	0x280000
File size:	562688 bytes
MD5 hash:	66CBE976594F666D5440264A4084B21F
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: 00000000.00000002.287974260.0000000002761000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.290045970.0000000003769000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.290045970.0000000003769000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2964 Parent PID: 4252

General

Start time:	16:50:01
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\aUkURZiJ" /XML "C:\Users\user\AppData\Local\Temp\tmp8923.tmp
Imagebase:	0x1270000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3336 Parent PID: 2964

General

Start time:	16:50:02
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe PID: 4792 Parent PID: 4252

General

Start time:	16:50:03
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\new order TRICOLOR-6.45 TRICOLOR-6.3 TRICOLOR-8.1 TRICOLOR-7.66.....exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa30000
File size:	562688 bytes
MD5 hash:	66CBE976594F666D5440264A4084B21F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.282084634.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.282084634.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.283151659.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.283151659.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.517392444.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.517392444.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.284209429.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.284209429.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.284592595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.284592595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.523008375.0000000002DB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.523008375.0000000002DB1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis