ID: 323773
Sample Name:
Arrivalnotice2020pdf.exe
Cookbook: default.jbs
Time: 14:24:11
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

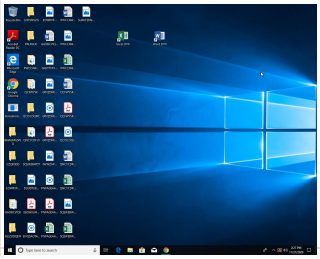
Analysis Report Arrivalnotice2020pdf.exe

Overview

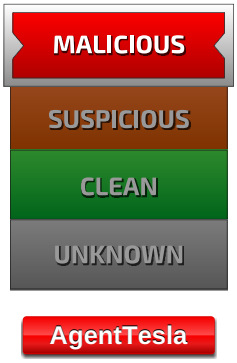
General Information

Sample Name:	Arrivalnotice2020pdf.exe
Analysis ID:	323773
MD5:	ed6f9a5ace6367f..
SHA1:	5ed4fd1e8a4e7db.
SHA256:	df107977e924659.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

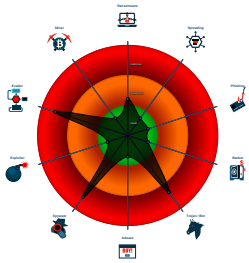


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Yara detected AgentTesla
- .NET source code contains very larg…
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- May check the online IP address of …
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- Arrivalnotice2020pdf.exe (PID: 5492 cmdline: 'C:\Users\user\Desktop\Arrivalnotice2020pdf.exe' MD5: ED6F9A5ACE6367F4E532DD4EC40762AC)
  - conhost.exe (PID: 1304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 2540 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "zSmwx",
  "URL: ": "https://dBHeYNWtul3f.net",
  "To: ": "akannwater@gmail.com",
  "ByHost: ": "webmail.hapkidocollege.com.au:587",
  "Password: ": "pXS5n2E1Xj",
  "From: ": "train@hapkidocollege.com.au"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.211934436.00000000000D3000.00000004.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.474831985.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Arrivalnotice2020pdf.exe PID: 5492	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: MSBuild.exe PID: 2540	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Unpacked PEs

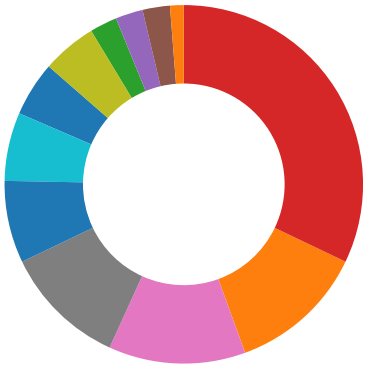
Source	Rule	Description	Author	Strings
3.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Arrivalnotice2020pdf.exe.b0000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: MSBuild connects to smtp port

Signature Overview



- AV Detection
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Copyright null 2020

Malware Analysis System Evasion:

- Found evasive API chain (trying to detect sleep duration tampering with parallel thread)
- 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)

HIPS / PFW / Operating System Protection Evasion:

- Maps a DLL or memory area into another process
- Writes to foreign memory regions

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:

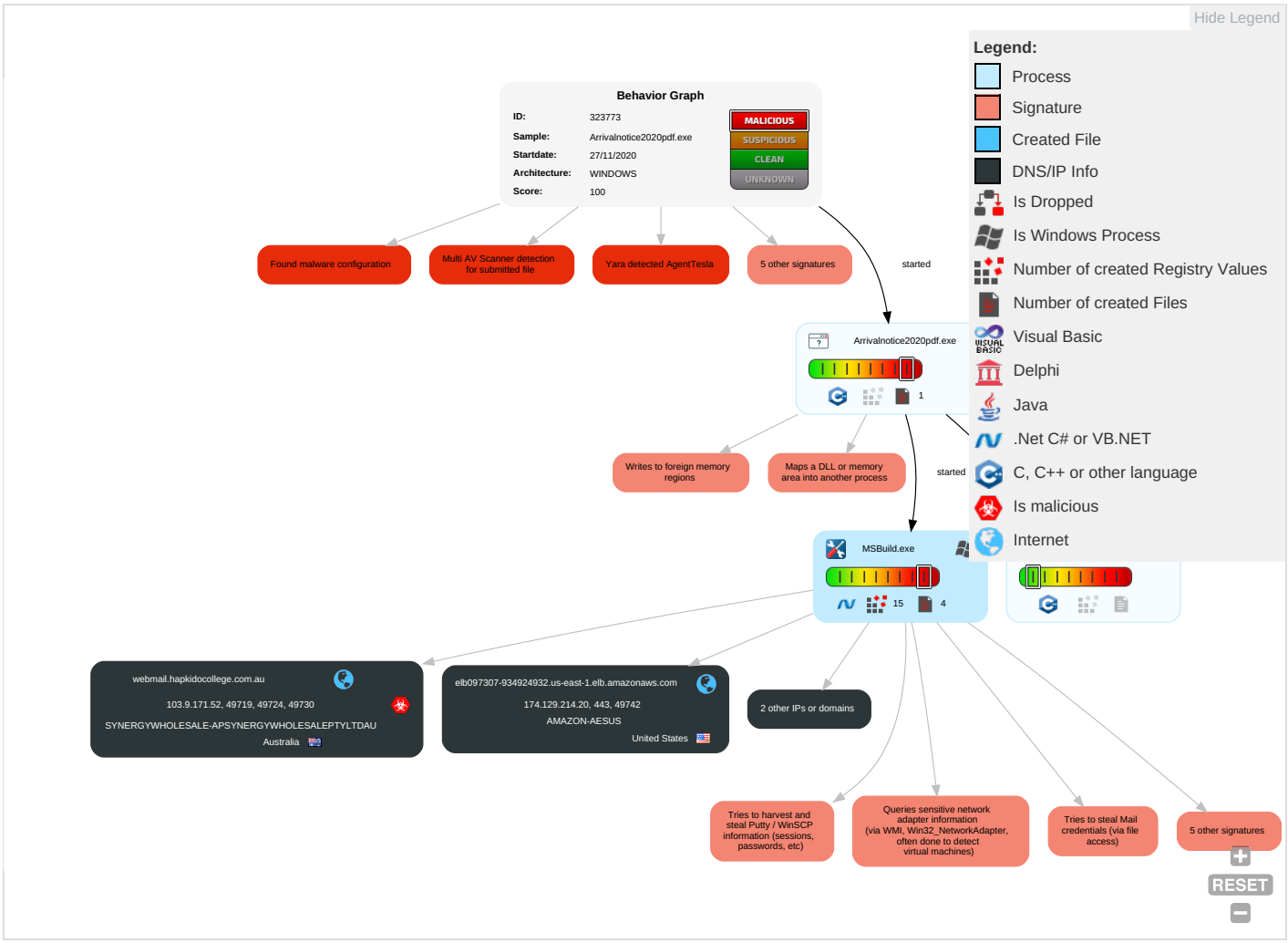
- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1 1	System Information Discovery 1 3 5	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 2 1 2	Obfuscated Files or Information 2	Credentials in Registry 1	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 1	NTDS	Security Software Discovery 1 4 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 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 2 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protc

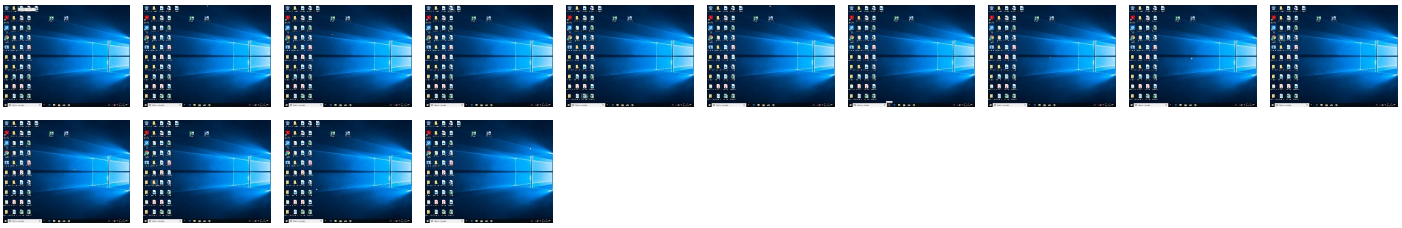
Behavior Graph



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
Arrivalnotice2020pdf.exe	23%	Virustotal		Browse
Arrivalnotice2020pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.MSBuild.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	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://dBHeYNWtul3f.net	0%	Avira URL Cloud	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://api.ipify.orgx&	0%	Avira URL Cloud	safe	
http://ZLVZGU.com	0%	Avira URL Cloud	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

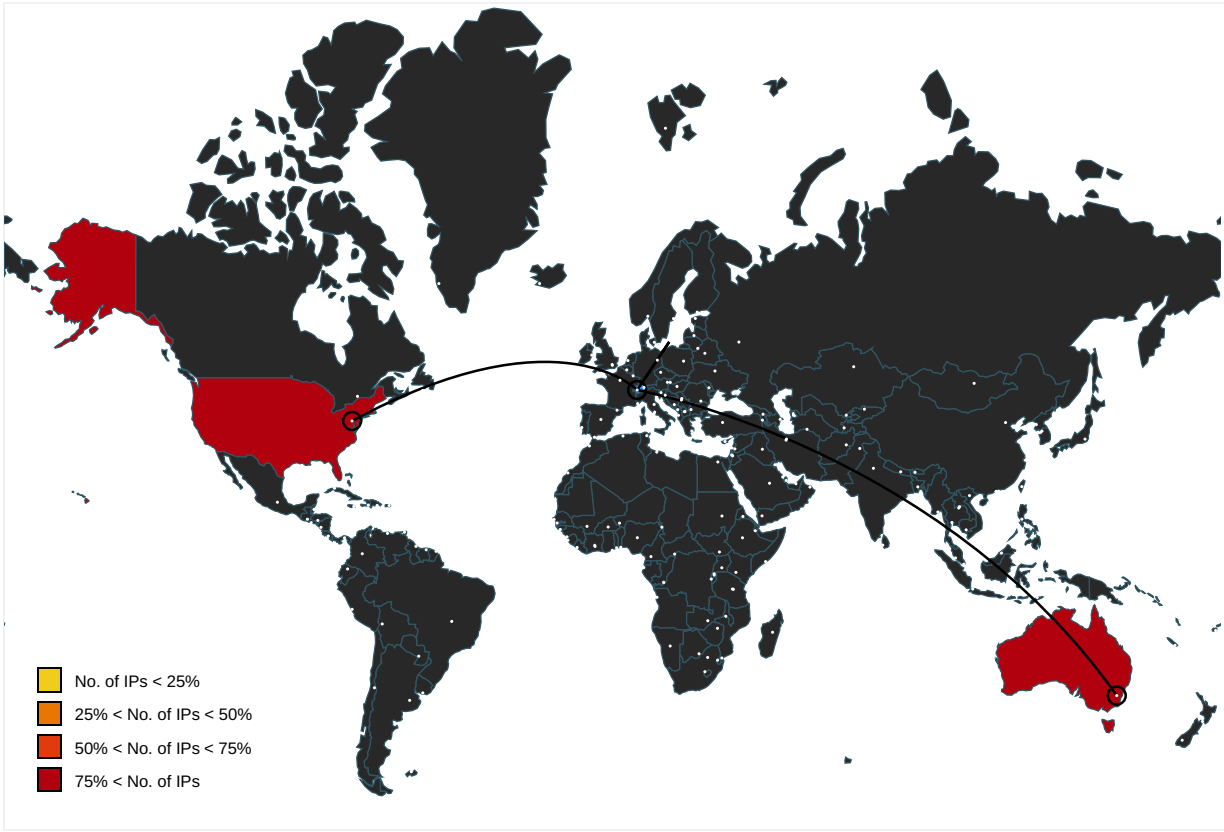
Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	174.129.214.20	true	false		high
webmail.hapkidocollege.com.au	103.9.171.52	true	true		unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dBHeYNWtul3f.net	MSBuild.exe, 00000003.00000002.479039341.000000000364E000.00000004.00000001.sdmp, MSBuild.exe, 00000003.00000002.479119119.0000000003668000.00000004.00000001.sdmp, MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	Arrivalnotice2020pdf.exe, 00000000.00000002.211934436.0000000000D3000.00000004.00020000.sdmp, MSBuild.exe, 00000003.00000002.474831985.0000000000402000.00000040.00000001.sdmp	false		high
http://https://api.ipify.orgx&	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ZLVZGU.com	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	MSBuild.exe, 00000003.00000003.409109256.000000000791A000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Arrivalnotice2020pdf.exe, MSBuild.exe, 00000003.00000002.474831985.0000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org/(	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	MSBuild.exe, 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.9.171.52	unknown	Australia		45638	SYNERGYWHOLESALE-APSYNERGYWHOLESALE PTYLTDAU	true
174.129.214.20	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323773
Start date:	27.11.2020
Start time:	14:24:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false

Copyright null 2020

Report type:	light
Sample file name:	Arrivalnotice2020pdf.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:	23
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@4/0@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 87.8% (good quality ratio 82.4%) • Quality average: 81.9% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 52.147.198.201, 104.42.151.234, 51.104.139.180, 23.210.248.85, 20.54.26.129, 8.241.122.254, 8.248.115.254, 8.253.95.249, 8.253.204.121, 67.26.137.254, 51.104.144.132, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • 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.

Simulations

Behavior and APIs

Time	Type	Description
14:25:10	API Interceptor	746x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
174.129.214.20	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• api.ipify.org/
	vQau1zZe6u.exe	Get hash	malicious	Browse	• api.ipify.org/
	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6containe r..exe	Get hash	malicious	Browse	• api.ipify.org/
	1119_673423.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	35WF7sZ7IR.exe	Get hash	malicious	Browse	• api.ipify.org/
	FACTURA.PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	Amended PO4800.exe	Get hash	malicious	Browse	• api.ipify.org/
	ScanDocuments202011PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	Commercial Invoice73802,PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	QUOTE.exe	Get hash	malicious	Browse	• api.ipify.org/
	1102905893.doc	Get hash	malicious	Browse	• api.ipify.org/
	1PmYoQcjTf.exe	Get hash	malicious	Browse	• api.ipify.org/
	uHrRcraZmP.exe	Get hash	malicious	Browse	• api.ipify.org/
	qIFdMHzqoE.exe	Get hash	malicious	Browse	• api.ipify.org/
	QZ0gaAlf0Z.exe	Get hash	malicious	Browse	• api.ipify.org/
	XTS QT-00572 REV_ASME NAMEPLATE MATERIAL Spec_scanned from a xerox printer001.exe	Get hash	malicious	Browse	• api.ipify.org/
	New Order_40981.exe	Get hash	malicious	Browse	• api.ipify.org/
	CHIBYKE08.exe	Get hash	malicious	Browse	• api.ipify.org/
	vT444moDbD.exe	Get hash	malicious	Browse	• api.ipify.org/
	PRODUCT SPECIFICATIONS.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	lxpo.exe	Get hash	malicious	Browse	• 54.204.14.42
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	SecuriteInfo.com.Variant.Bulz.233365.3916.exe	Get hash	malicious	Browse	• 23.21.252.4
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 54.225.169.28
	INVOICE.xlsx	Get hash	malicious	Browse	• 54.204.14.42
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	1125_56873981.doc	Get hash	malicious	Browse	• 54.243.161.145
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 54.235.142.93
	ER mexico.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 54.243.164.148
	SecuriteInfo.com.BackDoor.SpyBotNET.25.6057.exe	Get hash	malicious	Browse	• 50.19.252.36
	SecuriteInfo.com.BackDoor.SpyBotNET.25.7042.exe	Get hash	malicious	Browse	• 23.21.42.25

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SYNERGYWHOLESALE-APSYNERGYWHOLESALEPTYLTDAU	qpFvMReV7S.exe	Get hash	malicious	Browse	• 103.42.108.46
	zisuzZpoW2.exe	Get hash	malicious	Browse	• 103.27.32.34
	HMNo45VSzL.xls	Get hash	malicious	Browse	• 112.140.180.17
	http://benhams.info/backups/invoice/	Get hash	malicious	Browse	• 223.130.27.213
	Account update for your HDFC Bank.exe	Get hash	malicious	Browse	• 223.130.27.10
	PDF FILE.exe	Get hash	malicious	Browse	• 223.130.27.10

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	H4A2_423.EXE	Get hash	malicious	Browse	• 103.27.32.34
	http://pinksheep.com/opencart/eRjcgIxS/&d=DwIFaQ	Get hash	malicious	Browse	• 223.130.27.125
	http://pinksheep.com/opencart/eRjcgIxS/&d=DwIFaQ	Get hash	malicious	Browse	• 223.130.27.125
	http://pinksheep.com/opencart/eRjcgIxS/	Get hash	malicious	Browse	• 223.130.27.125
	SC# 84979926 Cargo Delivery .PDF.exe	Get hash	malicious	Browse	• 223.130.27.10
	REP_IDT_070120_BOR_073020.doc	Get hash	malicious	Browse	• 103.9.171.8
	REP_IDT_070120_BOR_073020.doc	Get hash	malicious	Browse	• 103.9.171.8
	83163251.doc	Get hash	malicious	Browse	• 103.9.171.8
	753200739936864412.doc	Get hash	malicious	Browse	• 103.9.171.8
	83163251.doc	Get hash	malicious	Browse	• 103.9.171.8
	N_ME9604945610TR.doc	Get hash	malicious	Browse	• 103.9.171.8
	753200739936864412.doc	Get hash	malicious	Browse	• 103.9.171.8
	P_PB3183494383ZD.doc	Get hash	malicious	Browse	• 103.9.171.8
	K_NXE_070120_IBB_073020.doc	Get hash	malicious	Browse	• 103.9.171.8
AMAZON-AESUS	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 3.215.226.95
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 54.83.52.76
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	http://https://webnavigator.co/?adprovider=AppFocus1&source=d-cp11560482685&group=cg60&device=c&keyword=&creative=477646941053&adposition=none&placement=www.123homeschool4me.com&target=segment_be_a_7802457135858218830&sl=&caid=11560482685&gw=1&test=%3a%2f%2fmail	Get hash	malicious	Browse	• 54.90.26.145
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0Nlk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0lnkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8l8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLlvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUlj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.236.142.3
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJIEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMIL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2Bl4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 23.20.225.204
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 52.2.188.208
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 52.205.236.122

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	http://searchlf.com	Get hash	malicious	Browse	• 34.196.190.195

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 174.129.214.20
	guy1.exe	Get hash	malicious	Browse	• 174.129.214.20
	guy2.exe	Get hash	malicious	Browse	• 174.129.214.20
	Exodus.exe	Get hash	malicious	Browse	• 174.129.214.20
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	#A06578987.xlsm	Get hash	malicious	Browse	• 174.129.214.20
	Order 51897.exe	Get hash	malicious	Browse	• 174.129.214.20
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	98650107.pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	Izezma64.dll	Get hash	malicious	Browse	• 174.129.214.20
	fuxenm32.dll	Get hash	malicious	Browse	• 174.129.214.20
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 174.129.214.20
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 174.129.214.20
	ER mexico.exe	Get hash	malicious	Browse	• 174.129.214.20
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 174.129.214.20
	SecuriteInfo.com.BackDoor.SpyBotNET.25.6057.exe	Get hash	malicious	Browse	• 174.129.214.20
	SecuriteInfo.com.ArtemisTrojan.exe	Get hash	malicious	Browse	• 174.129.214.20
	SecuriteInfo.com.BackDoor.SpyBotNET.25.7042.exe	Get hash	malicious	Browse	• 174.129.214.20
	SecuriteInfo.com.BackDoor.SpyBotNET.25.30157.exe	Get hash	malicious	Browse	• 174.129.214.20

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.366904859461942
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Arrivalnotice2020pdf.exe
File size:	387584
MD5:	ed6f9a5ace6367f4e532dd4ec40762ac
SHA1:	5ed4fd1e8a4e7dbed31928c2b7dd2ca1043cb68e
SHA256:	df107977e92465958c206bf42e33ce394e8573da3c4035b69bfa0d0eaf367914
SHA512:	e9315f1a9d8f0f8ddb0c48f08c8262af5a49937e11f57341d34cdd1ae3c945aec156faf7818e4a30cb61e82168e422e8ef697d1b9f74e9e31787aeea6d14d143
SSDEEP:	6144:3H5RPXz5XmxrAtJPsorVF3obF8V33f35XHC5UelMPBevP/539VI7hv9u998Q:X5RfzJmxrkBsor7aF8V33h3lerf5s7h6

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Km..Km..Km....>.Rm....<..m....=..m..Km...m....J.Xm..l. .Jm..l.:.Jm..Kmd.Jm..l.?.Jm..RichKm.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40482f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC0F239 [Fri Nov 27 12:34:01 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	be74bcf76a56fe7a35a0a7f280acf926

Entrypoint Preview

Instruction
call 00007FBDFC823183h
jmp 00007FBDFC81BA5Ch
call 00007FBDFC821DE7h
mov edx, eax
mov eax, dword ptr [edx+6Ch]
cmp eax, dword ptr [0041FC94h]
je 00007FBDFC81BBE2h
mov ecx, dword ptr [0041FD54h]
test dword ptr [edx+70h], ecx
jne 00007FBDFC81BBD7h
call 00007FBDFC821BCCh
mov eax, dword ptr [eax+04h]
ret
call 00007FBDFC821DC1h
mov edx, eax
mov eax, dword ptr [edx+6Ch]
cmp eax, dword ptr [0041FC94h]
je 00007FBDFC81BBE2h
mov ecx, dword ptr [0041FD54h]
test dword ptr [edx+70h], ecx
jne 00007FBDFC81BBD7h
call 00007FBDFC821BA6h
add eax, 000000A0h
ret
push ebp
mov ebp, esp
sub esp, 44h
mov eax, dword ptr [0041F9B8h]
xor eax, ebp

Copyright null 2020

Instruction
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
mov dword ptr [ebp-2Ch], ebx
mov eax, dword ptr [esi+000000A8h]
mov dword ptr [ebp-20h], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-44h], esi
mov dword ptr [ebp-40h], ebx
test eax, eax
je 00007FBDFC81BEE2h
push edi
lea edi, dword ptr [esi+04h]
cmp dword ptr [edi], ebx
jne 00007FBDFC81BBEEh
push edi
push 00001004h
push eax
lea eax, dword ptr [ebp-44h]
push ebx
push eax
call 00007FBDFC822648h
add esp, 14h
test eax, eax
jne 00007FBDFC81BE8Ah
push 00000004h
call 00007FBDFC81EFB5h
push 00000002h
push 00000180h
mov dword ptr [ebp-2Ch], eax

Rich Headers

Programming Language:	• [RES] VS2012 build 50727 • [LNK] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d868	0xc8	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5c000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5d000	0x1484	.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	0x1c520	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x204	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16129	0x16200	False	0.572199417373	data	6.66397370775	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x18000	0x63ba	0x6400	False	0.363125	data	4.85831029815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x3c884	0x39a00	False	0.978422417299	data	7.96878633663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5c000	0x1e0	0x200	False	0.53125	data	4.71767883295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5d000	0x8350	0x8400	False	0.127811316288	data	1.58596756783	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x5c060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	HeapReAlloc, EnumSystemLocalesEx, IsValidLocaleName, LCMapStringEx, GetUserDefaultLocaleName, GetModuleHandleW, TerminateProcess, GetCurrentProcess, LoadLibraryExW, FlsSetValue, FlsGetValue, FlsAlloc, SetUnhandledExceptionFilter, UnhandledExceptionFilter, SetFilePointerEx, ReadFile, GetConsoleMode, GetConsoleCP, FlushFileBuffers, CloseHandle, GetOEMCP, GetACP, IsValidCodePage, FreeEnvironmentStringsW, OutputDebugStringW, LoadLibraryW, SetStdHandle, WriteConsoleW, ReadConsoleW, CreateFileW, VirtualProtect, FlsFree, GetEnvironmentStringsW, GetTickCount64, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetModuleFileNameA, GetStartupInfoW, InitOnceExecuteOnce, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, EncodePointer, DecodePointer, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, Sleep, GetLocaleInfoEx, MultiByteToWideChar, GetStringTypeW, GetLastError, HeapFree, GetCommandLineA, GetCPInfo, RaiseException, RtlUnwind, HeapAlloc, InitializeCriticalSectionAndSpinCount, IsProcessorFeaturePresent, IsDebuggerPresent, GetProcessHeap, SetLastError, GetCurrentThreadId, ExitProcess, GetModuleHandleExW, GetProcAddress, HeapSize, GetStdHandle, WriteFile, GetModuleFileNameW, GetFileType
MSWSOCK.dll	s_perror, rexec, rcmd, GetNameByTypeW, EnumProtocolsW, dn_expand
SETUPAPI.dll	SetupQueryInfFileInformationW, SetupGetInfFileListA, SetupQueueDeleteA
MPR.dll	MultinetGetConnectionPerformanceA, WNetConnectionDialog1A, WNetGetResourceParentA, MultinetGetConnectionPerformanceW, WNetGetUserW
WINMM.dll	timeEndPeriod, timeKillEvent, mmioFlush, midiStreamOut, joySetCapture, midiInStart
pdh.dll	PdhVbGetCounterPathElements, PdhRemoveCounter, PdhEnumObjectItemsW, PdhOpenQueryA, PdhVbIsGoodStatus, PdhGetLogFileSize
msi.dll	
GDI32.dll	SetMagicColors, EnumFontFamiliesExW, CreateRectRgn, RemoveFontMemResourceEx, EudcUnloadLinkW, CreateCompatibleBitmap, CreateFontIndirectA, ScaleViewportExtEx, CreatePatternBrush, CreateICW
MAPI32.dll	

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 81

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:24:55.405668974 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.425780058 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.443604946 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.443954945 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.444000006 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.444039106 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.444077969 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.444089890 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.444113970 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.444125891 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.444180965 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.455045938 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.455089092 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.455174923 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.455215931 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.455785036 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.455822945 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.455879927 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.455908060 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.457230091 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.457493067 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.457535028 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.457590103 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.457617998 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.459353924 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.459453106 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.501156092 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.501204967 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.501315117 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.501358032 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.537703991 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.576322079 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.576375961 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.576575994 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.576625109 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.577052116 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.577094078 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.577122927 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.577147961 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.578737020 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.578814030 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.578825951 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.578875065 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.580406904 CET	443	49702	92.122.145.220	192.168.2.3

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:24:55.580508947 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.588928938 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.606633902 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.617360115 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.617413998 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.617547035 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.617574930 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.618076086 CET	443	49697	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.618172884 CET	49697	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.652687073 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.652846098 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.653779030 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.653856039 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.653902054 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.653932095 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.653975964 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.653994083 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.655035019 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.655101061 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.655152082 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.655169964 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.656676054 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.656740904 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.656774044 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.656805038 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.658318996 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.658385992 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.658420086 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.658451080 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.659981012 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.660054922 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.660087109 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.660115957 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.661645889 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.661709070 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.661746025 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.661767960 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.663324118 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.663403988 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.663441896 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.663544893 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.664993048 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.665066004 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.665108919 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.665132046 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.666649103 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.666721106 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.666760921 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.666817904 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.668351889 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.668418884 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.668459892 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.668497086 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.669945002 CET	443	49702	92.122.145.220	192.168.2.3
Nov 27, 2020 14:24:55.670032024 CET	49702	443	192.168.2.3	92.122.145.220
Nov 27, 2020 14:24:55.813956976 CET	49702	443	192.168.2.3	92.122.145.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:25:04.670833111 CET	60152	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:04.698086977 CET	53	60152	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:05.383215904 CET	57544	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:05.410538912 CET	53	57544	8.8.8.8	192.168.2.3

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 14:25:06.052160978 CET	55984	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:06.087801933 CET	53	55984	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:06.782588005 CET	64185	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:06.809679985 CET	53	64185	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:07.517072916 CET	65110	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:07.544064999 CET	53	65110	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:08.183290005 CET	58361	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:08.210572004 CET	53	58361	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:08.902954102 CET	63492	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:08.930222034 CET	53	63492	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:09.579035997 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:09.606163025 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:10.332566023 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:10.359648943 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:11.325078964 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:11.352227926 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:12.437009096 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:12.475356102 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:27.735615015 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:27.762844086 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:28.137470007 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:28.175828934 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:39.478696108 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:40.244265079 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:42.993508101 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:43.819489956 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:43.846821070 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:43.982381105 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:44.009459019 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:44.648421049 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:44.675628901 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:45.610944986 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:45.638127089 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:50.721287012 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:50.748570919 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:52.535218000 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:52.562628984 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:53.285748959 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:53.312868118 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:54.105633020 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:54.141134977 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 14:25:55.094934940 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:25:55.122128963 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 14:26:01.857494116 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:26:01.884722948 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 14:26:06.416886091 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:26:06.463174105 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 14:26:30.786530972 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:26:30.813698053 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 14:26:37.246206999 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:26:37.273241997 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 14:26:39.794296980 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 14:26:39.837749958 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 14:25:39.478696108 CET	192.168.2.3	8.8.8.8	0xdcfb	Standard query (0)	webmail.hapkidocollege.com.au	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.786530972 CET	192.168.2.3	8.8.8.8	0xb745	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)

DNS Answers

Copyright null 2020

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 14:25:40.244265079 CET	8.8.8.8	192.168.2.3	0xdcfb	No error (0)	webmail.hapkidocollege.com.au		103.9.171.52	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 14:26:30.813698053 CET	8.8.8.8	192.168.2.3	0xb745	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 14:26:31.051835060 CET	174.129.214.20	443	192.168.2.3	49742	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018	Sun Jan 24 00:59:59 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

SMTP Packets

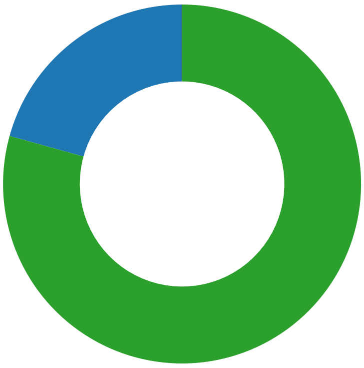
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 14:25:41.367238998 CET	587	49719	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:25:40 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:25:41.368335009 CET	49719	587	192.168.2.3	103.9.171.52	EHLO 632922
Nov 27, 2020 14:25:41.634421110 CET	587	49719	103.9.171.52	192.168.2.3	250-c5s3-4e-syd.hosting-services.net.au Hello 632922 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 14:25:41.634907961 CET	49719	587	192.168.2.3	103.9.171.52	AUTH login dHJhaW5AaGFwa2lkb2NvbGxlZ2UuY29tLmF1
Nov 27, 2020 14:25:42.231693029 CET	49719	587	192.168.2.3	103.9.171.52	AUTH login dHJhaW5AaGFwa2lkb2NvbGxlZ2UuY29tLmF1
Nov 27, 2020 14:25:42.934869051 CET	49719	587	192.168.2.3	103.9.171.52	AUTH login dHJhaW5AaGFwa2lkb2NvbGxlZ2UuY29tLmF1
Nov 27, 2020 14:25:43.755945921 CET	587	49719	103.9.171.52	192.168.2.3	334 UGFzc3dvcmQ6
Nov 27, 2020 14:25:44.048384905 CET	587	49719	103.9.171.52	192.168.2.3	235 Authentication succeeded
Nov 27, 2020 14:25:44.048794031 CET	49719	587	192.168.2.3	103.9.171.52	MAIL FROM:<train@hapkidocollege.com.au>
Nov 27, 2020 14:25:44.314590931 CET	587	49719	103.9.171.52	192.168.2.3	250 OK
Nov 27, 2020 14:25:44.317465067 CET	49719	587	192.168.2.3	103.9.171.52	RCPT TO:<akannwater@gmail.com>
Nov 27, 2020 14:25:44.657011032 CET	587	49719	103.9.171.52	192.168.2.3	250 Accepted
Nov 27, 2020 14:25:44.657308102 CET	49719	587	192.168.2.3	103.9.171.52	DATA
Nov 27, 2020 14:25:44.922913074 CET	587	49719	103.9.171.52	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 27, 2020 14:25:47.853806973 CET	587	49719	103.9.171.52	192.168.2.3	250 OK id=1kidkt-003UbD-Iv
Nov 27, 2020 14:25:49.862801075 CET	587	49724	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:25:48 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:25:49.866229057 CET	49724	587	192.168.2.3	103.9.171.52	EHLO 632922
Nov 27, 2020 14:25:50.129899979 CET	587	49724	103.9.171.52	192.168.2.3	250-c5s3-4e-syd.hosting-services.net.au Hello 632922 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 14:25:50.262506008 CET	587	49724	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:26:00.085405111 CET	587	49730	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:25:58 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:00.085947990 CET	49730	587	192.168.2.3	103.9.171.52	EHLO 632922
Nov 27, 2020 14:26:00.349783897 CET	587	49730	103.9.171.52	192.168.2.3	250-c5s3-4e-syd.hosting-services.net.au Hello 632922 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 14:26:00.356672049 CET	587	49730	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:26:10.958657980 CET	587	49739	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:26:09 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:10.958883047 CET	49739	587	192.168.2.3	103.9.171.52	EHLO 632922
Nov 27, 2020 14:26:11.222681046 CET	587	49739	103.9.171.52	192.168.2.3	250-c5s3-4e-syd.hosting-services.net.au Hello 632922 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 14:26:11.264421940 CET	587	49739	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 14:26:19.524956942 CET	587	49740	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:26:18 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:19.639858961 CET	587	49740	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:26:28.998317957 CET	587	49741	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:26:27 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:29.236226082 CET	587	49741	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:26:37.362380981 CET	587	49743	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:26:36 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:37.579276085 CET	587	49743	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:26:39.885345936 CET	587	49745	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:26:38 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:40.144205093 CET	587	49745	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:26:53.247958899 CET	587	49747	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:26:51 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:26:53.248662949 CET	49747	587	192.168.2.3	103.9.171.52	EHLO 632922
Nov 27, 2020 14:26:53.512720108 CET	587	49747	103.9.171.52	192.168.2.3	250-c5s3-4e-syd.hosting-services.net.au Hello 632922 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 14:26:53.513416052 CET	49747	587	192.168.2.3	103.9.171.52	AUTH login dHJhaW5AaGFwa2lkb2NvbGxlZ2UuY29tLmF1
Nov 27, 2020 14:26:53.778031111 CET	587	49747	103.9.171.52	192.168.2.3	334 UGFzc3dvcmQ6
Nov 27, 2020 14:26:54.061188936 CET	587	49747	103.9.171.52	192.168.2.3	235 Authentication succeeded
Nov 27, 2020 14:26:54.061547995 CET	49747	587	192.168.2.3	103.9.171.52	MAIL FROM:<train@hapkidocollege.com.au>
Nov 27, 2020 14:26:54.325247049 CET	587	49747	103.9.171.52	192.168.2.3	250 OK
Nov 27, 2020 14:26:54.325603008 CET	49747	587	192.168.2.3	103.9.171.52	RCPT TO:<akannwater@gmail.com>
Nov 27, 2020 14:26:54.678740025 CET	587	49747	103.9.171.52	192.168.2.3	250 Accepted
Nov 27, 2020 14:26:54.679126978 CET	49747	587	192.168.2.3	103.9.171.52	DATA
Nov 27, 2020 14:26:54.942570925 CET	587	49747	103.9.171.52	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 27, 2020 14:26:55.735517979 CET	49747	587	192.168.2.3	103.9.171.52	.
Nov 27, 2020 14:26:56.002332926 CET	587	49747	103.9.171.52	192.168.2.3	250 OK id=1kidm1-003UfT-Jb
Nov 27, 2020 14:27:06.204503059 CET	587	49747	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection
Nov 27, 2020 14:27:06.486670017 CET	587	49748	103.9.171.52	192.168.2.3	220-c5s3-4e-syd.hosting-services.net.au ESMTP Exim 4.93 #2 Sat, 28 Nov 2020 00:27:05 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 14:27:06.486910105 CET	49748	587	192.168.2.3	103.9.171.52	EHLO 632922
Nov 27, 2020 14:27:06.750746965 CET	587	49748	103.9.171.52	192.168.2.3	250-c5s3-4e-syd.hosting-services.net.au Hello 632922 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 14:27:06.768119097 CET	587	49748	103.9.171.52	192.168.2.3	421 c5s3-4e-syd.hosting-services.net.au lost input connection

Code Manipulations

Statistics

Behavior



- Arrivalnotice2020pdf.exe
- conhost.exe
- MSBuild.exe

Click to jump to process

System Behavior

Analysis Process: Arrivalnotice2020pdf.exe PID: 5492 Parent PID: 5648

General

Start time:	14:25:01
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\Arrivalnotice2020pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Arrivalnotice2020pdf.exe'
Imagebase:	0xb0000
File size:	387584 bytes
MD5 hash:	ED6F9A5ACE6367F4E532DD4EC40762AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.211934436.00000000000D3000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	D1186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	D1186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	D1186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	D1186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	D1186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	D1186	ReadFile

Analysis Process: conhost.exe PID: 1304 Parent PID: 5492

General

Start time:	14:25:01
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: MSBuild.exe PID: 2540 Parent PID: 5492

General

Start time:	14:25:02
Start date:	27/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Imagebase:	0xda0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000003.00000002.474831985.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.477291193.0000000003401000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5F91EDF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5F91EDF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	5F91EDF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	5F91EDF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5F91EDF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5F91EDF	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\9fbc83f3-30b2-4280-b208-53a19a8ea27a	unknown	4096	success or wait	1	5F91EDF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5F91EDF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5F91EDF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5F91EDF	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis