



ID: 365417
Cookbook: browseurl.jbs
Time: 15:12:26
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://covid19vaccine.hopto.org/new.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 13
Private 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 22
No static file info 22
Network Behavior 22
Network Port Distribution 22
TCP Packets 22
UDP Packets 24
DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 25
HTTP Packets 25
Code Manipulations 28
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: iexplore.exe PID: 4868 Parent PID: 792 28

Copyright Joe Security LLC 2021

General 28
File Activities 28
Registry Activities 28
Analysis Process: iexplore.exe PID: 2844 Parent PID: 4868 29
General 29
File Activities 29
Registry Activities 29
Analysis Process: EXCEL.EXE PID: 384 Parent PID: 792 29
General 29
File Activities 29
File Created 29
File Written 30
Registry Activities 30
Analysis Process: MSOSYNC.EXE PID: 1368 Parent PID: 384 30
General 30
File Activities 31
Registry Activities 31
Analysis Process: MSOSYNC.EXE PID: 4456 Parent PID: 384 31
General 31
File Activities 31
Registry Activities 31
Disassembly 31

Copyright Joe Security LLC 2021

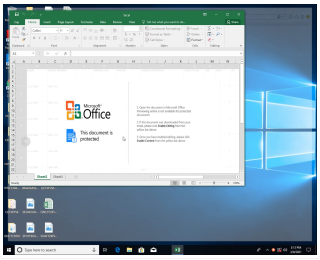
Analysis Report http://covid19vaccine.hopto.org/new.xlsx

Overview

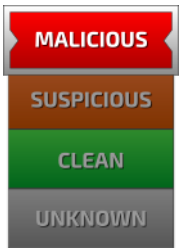
General Information

Sample URL:	http://covid19vaccine.hopto.org/new.xlsx
Analysis ID:	365417
Infos:	

Most interesting Screenshot:



Detection

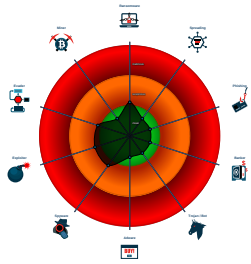


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Allocates a big amount of memory (p…
- Monitors certain registry keys / valu…
- Queries the volume information (nam…
- Tries to load missing DLLs

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4868 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2844 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4868 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- EXCEL.EXE (PID: 384 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - MSOSYNC.EXE (PID: 1368 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - MSOSYNC.EXE (PID: 4456 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

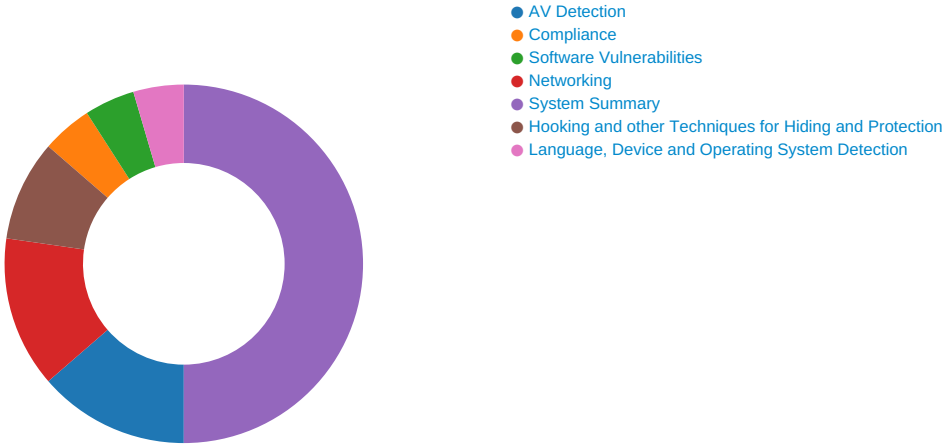
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

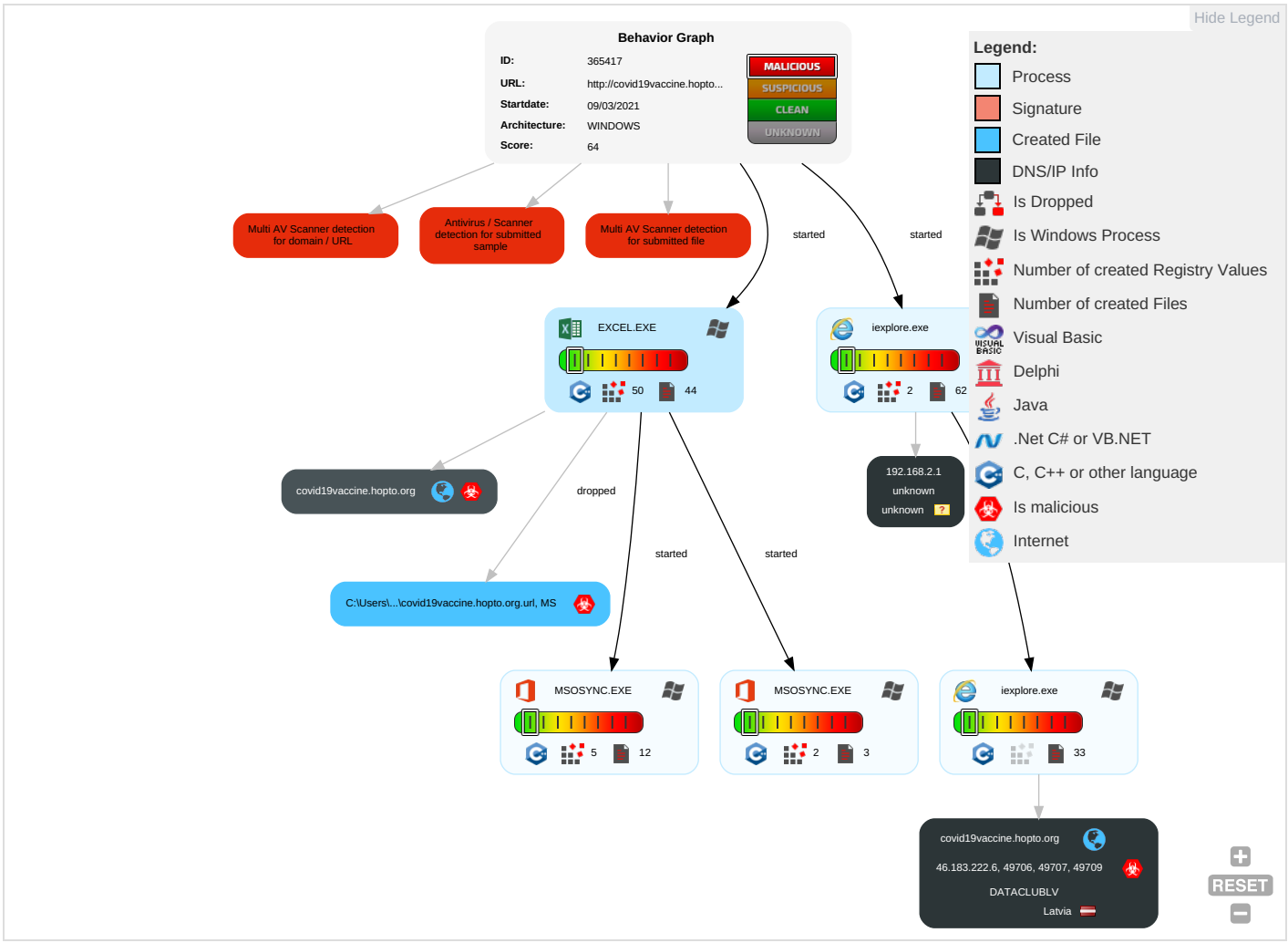
Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	DLL Side-Loading 1	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

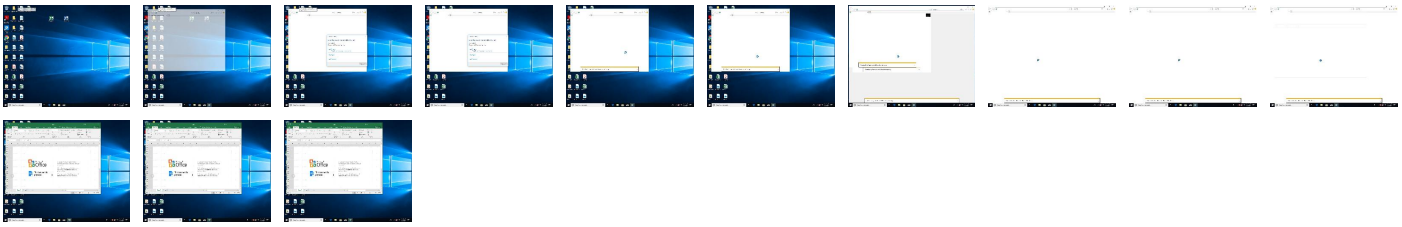
Behavior Graph

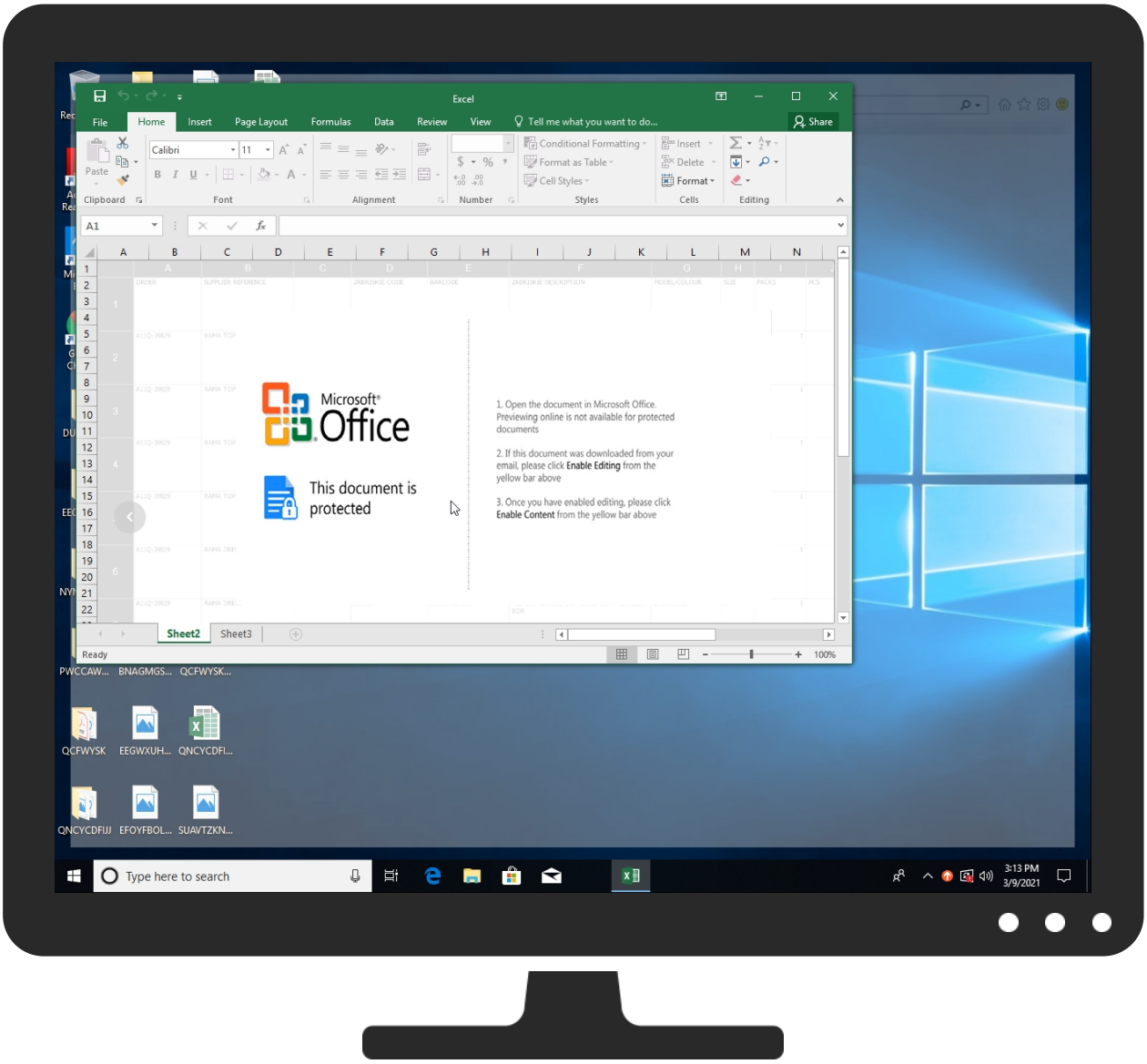


Screenshots

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
http://covid19vaccine.hopto.org/new.xlsx	15%	Virustotal		Browse
http://covid19vaccine.hopto.org/new.xlsx	100%	Avira URL Cloud	malware	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
covid19vaccine.hopto.org	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://covid19vaccine.hopto.org/	13%	Virustotal		Browse
http://covid19vaccine.hopto.org/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid19vaccine.hopto.org	46.183.222.6	true	true	• 13%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://covid19vaccine.hopto.org/new.xlsx	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://login.microsoftonline.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://shell.suite.office.com:1443	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://autodiscover-s.outlook.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://cdn.entity.	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://powerlift.acompli.net	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

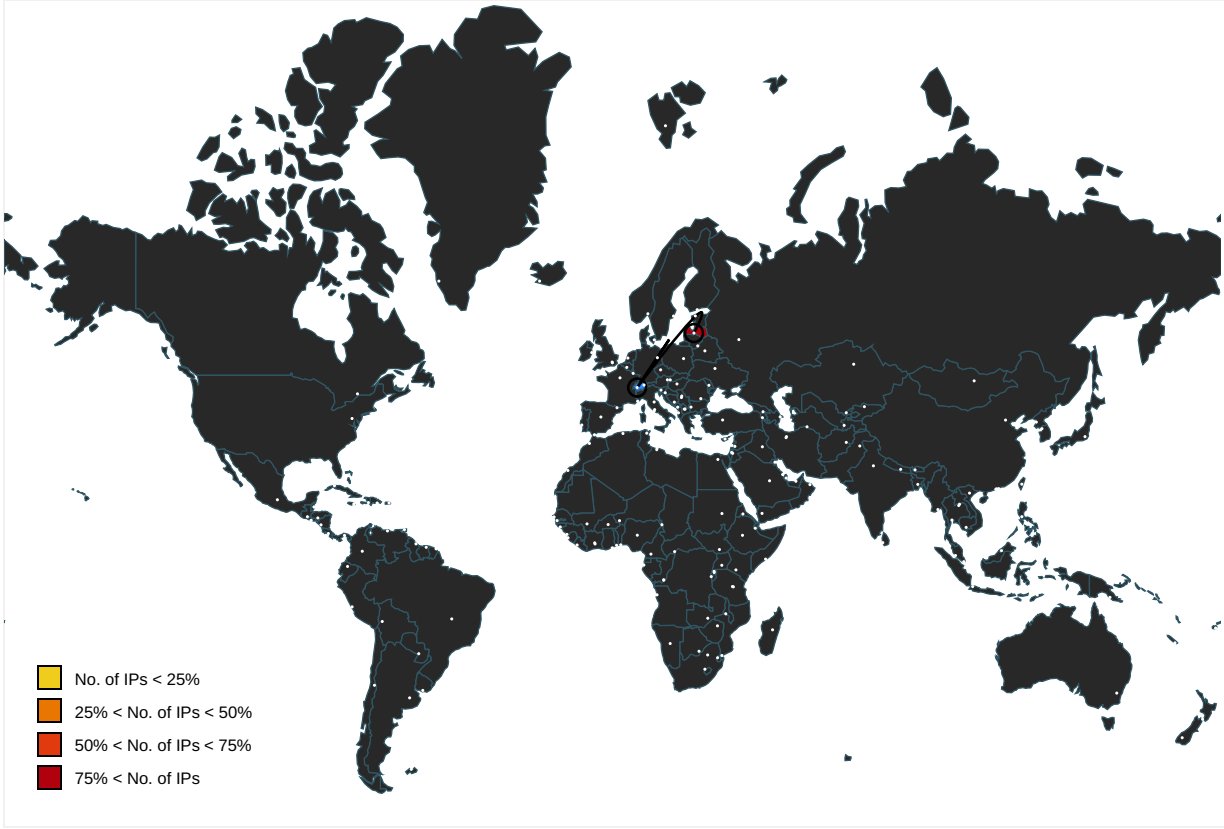
Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://cortana.ai	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://api.aadrm.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://api.microsoftstream.com/api/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://cr.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://ecs.office.com/config/v2/Office	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://covid19vaccine.hopto.org/	covid19vaccine.hopto.org.url.4.dr	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://graph.ppe.windows.net	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://officeci.azurewebsites.net/api/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://store.office.cn/addinstemplate	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://globaldisco.crm.dynamics.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://store.officeppe.com/addinstemplate	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.odwebp.svc.ms	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://web.microsoftstream.com/video/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://graph.windows.net	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://dataservice.o365filtering.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://ncus.contentsync.	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://weather.service.msn.com/data.aspx	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://apis.live.net/v5.0/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://management.azure.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://wus2.contentsync.	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://incidents.diagnostics.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://api.office.net	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://entitlement.diagnostics.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://outlook.office.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://templatelogging.office.com/client/log	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://outlook.office365.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://webshell.suite.office.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://management.azure.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://devnull.onenote.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://ncus.pagecontentsync.	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://messaging.office.com/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://augloop.office.com/v2	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://skyapi.live.net/Activity/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://dataservice.o365filtering.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false		high
http://https://directory.services.	E74F5F17-DC91-4EA1-89CD-4C485BA65FE2.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.183.222.6	covid19vaccine.hopto.org	Latvia		52048	DATACLUBLV	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365417
Start date:	09.03.2021
Start time:	15:12:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid19vaccine.hopto.org/new.xlsx
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:	30
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal64.win@8/24@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 52.255.188.83, 184.27.11.238, 52.109.88.177, 52.109.88.38, 52.109.12.23, 104.42.151.234, 184.30.20.56, 51.104.144.132, 93.184.221.240, 20.54.26.129, 20.82.209.183, 92.122.213.194, 92.122.213.247, 13.88.21.125, 13.64.90.137 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.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, e11290.dspg.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, nexus.officeapps.live.com, officeclient.microsoft.com, 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, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{03D92598-812D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	52824
Entropy (8bit):	1.9402306920184138
Encrypted:	false
SSDEEP:	192:rBZpZG2mW6tVifS8+zMHWBKwDiWBNyt18VjLzyQdLfg8KzMeVW/KQVMZSZA:rH/99SKjux9Iy/hZqN
MD5:	BFA61E073A013D54B2999FAD41FCCBAC
SHA1:	9E55604BBE8CDEA698E5DA3E60D6D36562484751
SHA-256:	14655D6E4E9069FE350DDC9B23346FCBA5C870400BD00DD1C0519B7DD7C38217
SHA-512:	AB7D434215FEBECC4F149BA74802A15A30C0959DAD6A4D7E725E833D10F3492D1CFC968EFF57477A9C286F0F142823DA227B5D048E8F3E83E4B53762B35AFDF C
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{03D9259A-812D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21080
Entropy (8bit):	1.6171426624248464
Encrypted:	false
SSDEEP:	48:IwlGcprUGwpagG4pQxGrapbShjGQpB6d3GHHpc6LITGUp8JIMG0pwJIlWTG8pG:r7ZsQA6BBSXjF2FWJlAaJIQA
MD5:	8C5B67F49F8E3D245F69B88EFCEC8FE4
SHA1:	38932AF71DE479E4692FCFA115A38C0C74835536
SHA-256:	8DD105833017ABD7C01519E284AC128C38E73277BBAF213C6E8832A883625E0C
SHA-512:	4D9CEFCCAD873EEF27CCED15136F2ABE38AA1341FCD0187F02FCA64E9DDBB9D0F4D441DC7082F3CFD932DC4EDC905C68366F61D2F1C1CD9A75C0DC5ECC6 6EB2
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0DBE67A1-812D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5842982116975501
Encrypted:	false
SSDEEP:	48:IwRGcprIGwpaGG4pQOGrapbSVGQpKKG7HpR3TGIpX2WGApm:rnZQQ26ABSfAlTFFxg
MD5:	B25EB353F675B1CCC977ED941E5F378E
SHA1:	346E95A5C84359D67614F364AE1CBDDB1B157F98
SHA-256:	AA537E0D2A7B9616A6D28850784931316C72B6E60DED872DB5CC44609E23166E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0DBE67A1-812D-11EB-90E4-ECF4BB862DED}.dat	
SHA-512:	AE43DC7EDC354598BD959727FD9C7326E0DA906401BDBCEED80A4E8249C9EEAFAD257D30583A4DBC1FFA18F13520F4122D961023FA1CAF126AFED40F3702D F5
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	626709
Entropy (8bit):	0.5038351839725628
Encrypted:	false
SSDEEP:	384:SgRJCw8SFH4fZ0jGBDq3nAWwwtZ1IG+hVZO4Fp2bWGTHi59:XCwHoZxGnzw/FqTH+9
MD5:	E1A2214070C982E66B59D8F94CF48888
SHA1:	ADA7D6F3EB3BD9F7B0E37D5DE9D34597ECB0030A
SHA-256:	29B6D254733F8EB3B2547CABD6E864CE50845BA33B648B4886A905E62C777C91
SHA-512:	EC668F1EB7101AD584063DB016A57AB0156AEEDE6EEE9FB04CE7CD0C8DCFD93035BD13D247FD48B7C0627D81015C9D38F0F306A42A94AE4D70A115183792C7 7
Malicious:	false
Reputation:	low
Preview:	.....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...NnW.7.....(....`.8{6....X.C'..3..y[z.|*..|.....XA..x..f_...$.g..'D...e....F.x....-b.T...4.0..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false
SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Reputation:	low
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	1.3742409383951601
Encrypted:	false
SSDEEP:	3:T/VFaV:ru
MD5:	3244B7E4BBA73F22865AA7A2C4DFEFE3
SHA1:	DF369D2C17D9B4A4AE2E0168DB2DF20F8C28D4B7
SHA-256:	D1DE38D56CD5D71F94105AA8B52CF5A2AA1FB224F8C531DE3D8DD569183A9896
SHA-512:	B456F19EBB5EBFC7D60DA958CAA1F2BD846A9FDB196B4321B64660738B19F52424565448C8E03573466E06721FA281C081ED73C66073656F7CBAF50D7F54859B
Malicious:	false
Reputation:	low
Preview:	067773. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E74F5F17-DC91-4EA1-89CD-4C485BA65FE2	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E74F5F17-DC91-4EA1-89CD-4C485BA65FE2	
Category:	dropped
Size (bytes):	132843
Entropy (8bit):	5.375079255091923
Encrypted:	false
SSDEEP:	1536:ccQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:mcQ9DQW+zUXiK
MD5:	1A5A63A8A853308DE67F78413C71E377
SHA1:	3C0FFD99AA18E3D86F4011CDCAB0AEA7F5FDC978
SHA-256:	931BAC6D40A811748C9FA54B5D0A10C6C7BC7740EE37E06F0E06F56491854865
SHA-512:	1E6EFF413C90F26AF326F51C4F491E4381D57DC06CE9317BFD2CD56E8DD8831D38BD2DD94641AF552CBC02CF206C673DA4CFE5417D99BA6DAC8ED29038927A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-03-09T14:13:25">.. Build: 16.0.13908.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1734685F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;......_h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1A3C9969.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.8986749529648215
Encrypted:	false
SSDEEP:	3072:i34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:s4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	052BC85A55B7568EF566115374AC8389
SHA1:	35EAA71579443E84C22F301B20CC9054E2C2C457
SHA-256:	2BB630453D0F8AF075AF719E2A498875E82E66A9BB93410B3F9D91A49A379A16
SHA-512:	21B45162FDBB5928D1152DB1E6FD6EBCA38382E96EC36859040A614D735F01F1A678325BC4C6DB8BED55A31DF0B15913940D7C2BA22EBE59825A81389AB28B3D
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....+.D.+.....+.(.+. .NeU..+...+.....+...+..NeU..+...+. ....y\|Q..+...+. .....,...z\|Q.....X...%...7.....{ .@.....C.a.l.i.b.r.....4.+.X.....+...+..2uQ.....+...+.. {sQ....8.+,...dv.....%.....%.....%.....!.....I...c..."..... .....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\408626D4.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 433x116, frames 3
Category:	dropped
Size (bytes):	7988
Entropy (8bit):	7.913570812072164

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\408626D4.jpeg	
Encrypted:	false
SSDEEP:	192:5Vz/djYtdWIToSdC7PyN0XgP2xfbbbbb3TLwZ6epikSfOD3kUJbbbbbR:5x/QWK5NKxbULD3Vf
MD5:	60CD11F234818D75CC569B1729C45695
SHA1:	01449AFC0887AB133764C84EA9C5CC9A1C67BEA7
SHA-256:	4559DD7CA810FC9C12B9D3FB4958867E2CAA399661EDC0CA7F8EB1B01B51C274
SHA-512:	377991F7D487CAA42C649A87A584DE7FB84A032B9E83156C59A805DFAFA4A30F8449036F7A4660F8DF331D7A7C52E0142EBA36BFB766AC2244BAEC3BE58F1C83
Malicious:	false
Reputation:	low
Preview:	......JFIF.....((..&...!1!%)-1... 383,7(-.+.....+% %---+-/----/---------/2-------------------------.....t...."..... H..... !1.AQ....."RSa...2Tq...B..#4bs..3r...5Ct...$.....)..... Q..!R..1A.ab"q.B.....?..,f...H.I..KL.:..Z....^.R..4.r.x.F.....4.T.....2.1..T..y....Z..SsAkCl .L.p_N.4.5E]v.<TWrj....K....+.?j..A....gX..}.\j.A....ny...Q..U.<.....9@ ....O.Wg...^._9H.7/.....ZW.....Usvug.x.....G5..R"3l..$.....U.X/...0.....+4+..j<.f....1....v#.-;Dz4]L...gQ..... Xj..i?G..._p.....7|.N.g.D..F?CT.....^_G5:&.&.I9.n....IY...Q...r.&&.Du\6.....$.G.g....19.....h....9.....?s?e...3..c.x../....=..@v:..M+.j..CP..].db'.t.M..`...d...|..~.y...P...."|>.E.... .Y.+H.s=I.q.c..lT.....r..3.5..s.x..43.....r....Y..<...uDf2....T.t-[..R.-2A.q0.g.....:..q".@.....=.(^S...i.\@..18....^tlr..G@4.K...nh.I...`...G.M..R7^.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\58FD3802.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	2594816
Entropy (8bit):	**7.996785207969099**
Encrypted:	**true**
SSDEEP:	49152:iYCt6TcsRjhaV8KxwDswpoosyDK0T8eLiDbPUFN+E9HfMTsODU+51Qcw2cqMC+gw:tZDFaVLm3RBAeODbyNt5EQODUqMUiGo
MD5:	3E4C88072D1B2BE5FB2B8798569E12A4
SHA1:	57B6810605996A7476E01428BC1CF2B1D078C129
SHA-256:	11E061E90A3EBAC7A4478EAF00941612355D7C10A510C5100F3D5A6689950787
SHA-512:	E31DC1FA1AC04C75D2A6E0462B4C616B5578C06E08CC9DDF4A0DC399C584BEC8378C6D45B84219FCC4122BC2D09596E86AAB3719C77C1C092977BEF5B0221(0
Malicious:	false
Reputation:	low
Preview:	.....>.....(.....z.....|.....~.....z.....|.....~.....z.....|.....~..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A... B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\705DCD08.xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	2594816
Entropy (8bit):	**7.996785207969099**
Encrypted:	**true**
SSDEEP:	49152:iYCt6TcsRjhaV8KxwDswpoosyDK0T8eLiDbPUFN+E9HfMTsODU+51Qcw2cqMC+gw:tZDFaVLm3RBAeODbyNt5EQODUqMUiGo
MD5:	3E4C88072D1B2BE5FB2B8798569E12A4
SHA1:	57B6810605996A7476E01428BC1CF2B1D078C129
SHA-256:	11E061E90A3EBAC7A4478EAF00941612355D7C10A510C5100F3D5A6689950787
SHA-512:	E31DC1FA1AC04C75D2A6E0462B4C616B5578C06E08CC9DDF4A0DC399C584BEC8378C6D45B84219FCC4122BC2D09596E86AAB3719C77C1C092977BEF5B0221(0
Malicious:	false
Reputation:	low
Preview:	.....>.....(.....z.....|.....~.....z.....|.....~.....z.....|.....~..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A... B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7574A056.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7574A056.png	
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\84FC70C5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....b..v....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^..|g.U.4.G...#..A....*.....>.i .....E..._.....R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;.....Z{..^..>.....E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0I.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\navcancl[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2713
Entropy (8bit):	4.1712007174415895
Encrypted:	false
SSDEEP:	24:r3avxU5hzslVmVMeLmVMyHf63lboxMCLxvriN6LOAPAnQay78eLx5Tb87nVkEhML:upU0GVeLVGBXvrp4n/1a5TI7Ve/G79KX
MD5:	4BCFE9F8DB04948CDDB5E31FE6A7F984
SHA1:	42464C70FC16F3F361C2419751ACD57D51613CDF
SHA-256:	BEE0439FCF31DE76D6E2D7FD377A24A34AC8763D5BF4114DA5E1663009E24228
SHA-512:	BB0EF3D32310644285F4062AD5F27F30649C04C5A442361A5DBE3672BD8CB585160187070872A31D9F30B70397D81449623510365A371E73BDA580E00EEF0E4E
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/navcancl.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="res://ieframe.dll/ErrorPageTemplate.css" />.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.... <title>Navigation Canceled</title>.... <script src="res://ieframe.dll/errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="res://ieframe.dll /httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:navCancelInit(); ">.... <table width ="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rows pan="2">.. <img src="res://ieframe.dll/info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\new[1].xlsx	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	CDFV2 Encrypted
Category:	downloaded
Size (bytes):	2594816
Entropy (8bit):	**7.996785207969099**
Encrypted:	**true**
SSDEEP:	49152:iYCt6TcsRjhaV8KxwDswpoosyDK0T8eLiDbPUFN+E9HfMTsODU+51Qcw2cqMC+gw:tZDFaVLm3RBAeODbyNt5EQODUqMUiGo
MD5:	3E4C88072D1B2BE5FB2B8798569E12A4
SHA1:	57B6810605996A7476E01428BC1CF2B1D078C129
SHA-256:	11E061E90A3EBAC7A4478EAF00941612355D7C10A510C5100F3D5A6689950787
SHA-512:	E31DC1FA1AC04C75D2A6E0462B4C616B5578C06E08CC9DDF4A0DC399C584BEC8378C6D45B84219FCC4122BC2D09596E86AAB3719C77C1C092977BEF5B0221 0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\new[1].xlsx	
Malicious:	false
Reputation:	low
IE Cache URL:	http://covid19vaccine.hopto.org/new.xlsx
Preview:	.....>.....(.....z.....|.....~.....z.....|.....~.....z.....|.....~..... ....!..".#...$...%...&..'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.33509565644547
Encrypted:	false
SSDEEP:	3:oVXU0VQUNW8JOGXnE0bU4uULX+n:o9UfBqER4u7
MD5:	7D6293CE6E6EEED8EB71759FEF988094
SHA1:	59BBEC78A66D1A907E884F9EBEB4F9923FA74DED
SHA-256:	C0F15722C10506DE67CBE81B49630BD90C2EAFFACBD9C9F307D746414F1133C8
SHA-512:	313BE7A39A05FA699099D72011ED9BCDC7D9D6AC54A77ECBB030F085D391A70282DF05E57B093A2382341156D021F58DEAF1DF3653B1789B91397A789022891A
Malicious:	false
Reputation:	low
Preview:	[2021/03/09 15:13:12.175] Latest deploy version: ..[2021/03/09 15:13:12.191] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF1D7596480EE11CB0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34085
Entropy (8bit):	0.3295478042940685
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw6E9lw609l26q/9l2JX:kBqoxKAuvScS+6X6Z6q+JIcXJJI0Jlly
MD5:	0952478B45F3C900D8EE31DD93A65603
SHA1:	445544934E9F0CFCAB41E000F4A10A79D534EDFC
SHA-256:	C2C82F8963E96B5BFD17709770CB2FEF2712CB3FCB1BB231A06BA0BC6A78A3A4
SHA-512:	5E7FF58490C443F8E56BE64E44E03E2F2385592F0880F5B4FAE6FB9E5E73B247D48BD78E7C0F1AE429774FE711B74EAA16E9AF6933445AB08CFB4C04F7FEB1E9
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBF46033416D08F0A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13205
Entropy (8bit):	0.5965818802832725
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lofF9lo99lWcotsbhplrr:kBqoIGYcEsbhTH
MD5:	E52C3997C88D5A02E777116EF77FA728
SHA1:	5A4CA19E4D345ADDCE22E84215395F387CF5CBB3
SHA-256:	2726227E3CEE58E145761454F7EDA4C0CD4A4A30842A3015D22C39A345190B37
SHA-512:	16821E1ACBA9BC789C78BE47A073AE1541FE2C723E1372E8BD7B1A5FF4148A003FCE3D69E21353900804E9FC9202DA82C9509CEAA5E0BDDAA368723234C9EF5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEEFA64FCDCD02473.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29745
Entropy (8bit):	0.3850070054531315
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggy24blqU5:kBqoxxJhHWSVSEabytZqFZvJQ2y
MD5:	FB84E74C5861C33D808C729E9C664DEB
SHA1:	6DFE1B0ADBF07035FD18B8B6306759F58E60E934
SHA-256:	7EE577F7A9AD22B32C317EFB2C684B1CF74CBC767D9E3A03B49AD0061E3E7C18
SHA-512:	CA721A5257FACB0039D1023B062A89E3E00C8099817DC9E980D3C60F1E09258E84546230000EE6534E4B2601CC6E432B7D9426D54D5CEDC56FF46415E9C67777
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

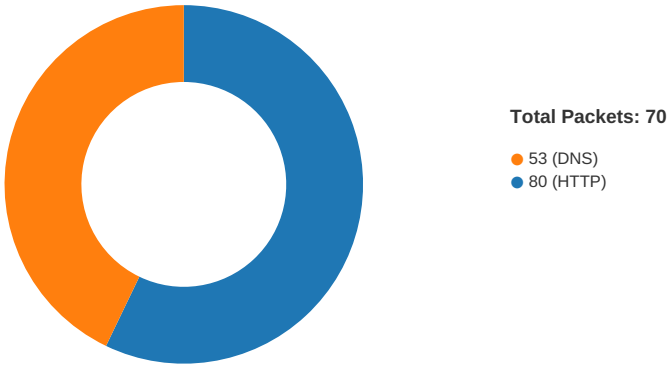
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\new.xlsx.url	
Malicious:	false
Reputation:	low
Preview:	[InternetShortcut]..URL=http://covid19vaccine.hopto.org/new.xlsx..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:13:13.260173082 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.261132956 CET	49707	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.328773022 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.328882933 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.330225945 CET	80	49707	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.330359936 CET	49707	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.334832907 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.403486013 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.403541088 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.403755903 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.470381975 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.470442057 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.470483065 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.470518112 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.470534086 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.470580101 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.470586061 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.470603943 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.540851116 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.540921926 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.540946007 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.540978909 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.541001081 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.541002989 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.541029930 CET	80	49706	46.183.222.6	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:13:13.541059017 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.541062117 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.541083097 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.541117907 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.541146994 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607037067 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607070923 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607088089 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607105017 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607122898 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607139111 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607155085 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607192039 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607189894 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607209921 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607244015 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607254982 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607266903 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607311964 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607317924 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607331038 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607348919 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607368946 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607378006 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607407093 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607424974 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607444048 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.607449055 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607496977 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.607530117 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.680778027 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.680800915 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.680813074 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.680826902 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.680846930 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.680886030 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.680947065 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.680979967 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.680999041 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681015968 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681031942 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681049109 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681057930 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681066990 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681104898 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681147099 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681174994 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681175947 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681193113 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681230068 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681233883 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681265116 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681269884 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681294918 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681303978 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681313992 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681344986 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681371927 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681396008 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681405067 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681436062 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681444883 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681462049 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681482077 CET	80	49706	46.183.222.6	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:13:13.681490898 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681514025 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681538105 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681543112 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681580067 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681591034 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681624889 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681626081 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681663036 CET	49706	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:13:13.681664944 CET	80	49706	46.183.222.6	192.168.2.3
Mar 9, 2021 15:13:13.681698084 CET	49706	80	192.168.2.3	46.183.222.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:13:04.530427933 CET	50620	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:04.564084053 CET	64938	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:04.582986116 CET	53	50620	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:04.611946106 CET	53	64938	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:12.139215946 CET	60152	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:12.198040009 CET	53	60152	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:13.190373898 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:13.247843027 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:25.228328943 CET	55984	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:25.284188986 CET	53	55984	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:25.700359106 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:25.758518934 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:26.697518110 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:26.752007008 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:27.728367090 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:27.782921076 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:29.727216959 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:29.783771992 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:30.153937101 CET	65110	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:30.213191986 CET	53	65110	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:30.409173012 CET	58361	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:30.411461115 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:30.463494062 CET	53	58361	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:30.466097116 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:31.398334980 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:31.444272041 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:32.429239035 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:32.483438969 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:33.727170944 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:33.781574011 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:34.432425976 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:34.488954067 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:36.056159973 CET	60831	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:36.104882002 CET	53	60831	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:38.482774973 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:38.542498112 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:43.493226051 CET	60100	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:43.521485090 CET	53195	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:43.547888041 CET	53	60100	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:43.576872110 CET	53	53195	8.8.8.8	192.168.2.3
Mar 9, 2021 15:13:59.744580030 CET	50141	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:13:59.802736044 CET	53	50141	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:04.295542002 CET	53023	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:04.365312099 CET	53	53023	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:07.685796976 CET	49563	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:07.731858015 CET	53	49563	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:20.717246056 CET	51352	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:20.765988111 CET	53	51352	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:25.718823910 CET	59349	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:14:25.778388023 CET	53	59349	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:39.722002029 CET	57084	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:39.776700974 CET	53	57084	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:47.954356909 CET	58823	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:48.000380993 CET	53	58823	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:56.027770042 CET	57568	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:56.073787928 CET	53	57568	8.8.8.8	192.168.2.3
Mar 9, 2021 15:14:57.590689898 CET	50540	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:14:57.659845114 CET	53	50540	8.8.8.8	192.168.2.3
Mar 9, 2021 15:15:09.433790922 CET	54366	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:15:09.482459068 CET	53	54366	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 15:13:13.190373898 CET	192.168.2.3	8.8.8.8	0x4efe	Standard query (0)	covid19vaccine.hopto.org	A (IP address)	IN (0x0001)
Mar 9, 2021 15:13:30.153937101 CET	192.168.2.3	8.8.8.8	0xbdc2	Standard query (0)	covid19vaccine.hopto.org	A (IP address)	IN (0x0001)
Mar 9, 2021 15:13:30.409173012 CET	192.168.2.3	8.8.8.8	0xec58	Standard query (0)	covid19vaccine.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 15:13:13.247843027 CET	8.8.8.8	192.168.2.3	0x4efe	No error (0)	covid19vaccine.hopto.org		46.183.222.6	A (IP address)	IN (0x0001)
Mar 9, 2021 15:13:30.213191986 CET	8.8.8.8	192.168.2.3	0xbdc2	No error (0)	covid19vaccine.hopto.org		46.183.222.6	A (IP address)	IN (0x0001)
Mar 9, 2021 15:13:30.463494062 CET	8.8.8.8	192.168.2.3	0xec58	No error (0)	covid19vaccine.hopto.org		46.183.222.6	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19vaccine.hopto.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49706	46.183.222.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:13:13.334832907 CET	878	OUT	GET /new.xlsx HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: covid19vaccine.hopto.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:13:13.403486013 CET	879	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:13:11 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2 Last-Modified: Tue, 02 Mar 2021 09:12:03 GMT ETag: "279800-5bc8a20abf075" Accept-Ranges: bytes Content-Length: 2594816 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet Data Raw: d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 28 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fe ff ff ff 00 00 00 00 00 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 ff 07 00 00 80 08 00 00 f9 08 00 00 7a 09 00 00 fb 09 00 00 7c 0a 00 00 fd 0a 00 00 7e 0b 00 00 ff 0b 00 00 80 0c 00 00 f9 0c 00 00 7a 0d 00 00 fb 0d 00 00 7c 0e 00 00 fd 0e 00 00 7e 0f 00 00 ff 0f 00 00 80 10 00 00 f9 10 00 00 7a 11 00 00 fb 11 00 00 7c 12 00 00 fd 12 00 00 7e 13 00 00 ff ff ff

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:13:30.831020117 CET	3661	OUT	HEAD /new.xlsx HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Excel 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: covid19vaccine.hopto.org
Mar 9, 2021 15:13:30.899379969 CET	3661	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:13:29 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2 Last-Modified: Tue, 02 Mar 2021 09:12:03 GMT ETag: "279800-5bc8a20abf075" Accept-Ranges: bytes Content-Length: 2594816 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Mar 9, 2021 15:13:33.942971945 CET	3662	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Excel 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: covid19vaccine.hopto.org
Mar 9, 2021 15:13:34.013942003 CET	3662	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:13:32 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: httpd/unix-directory

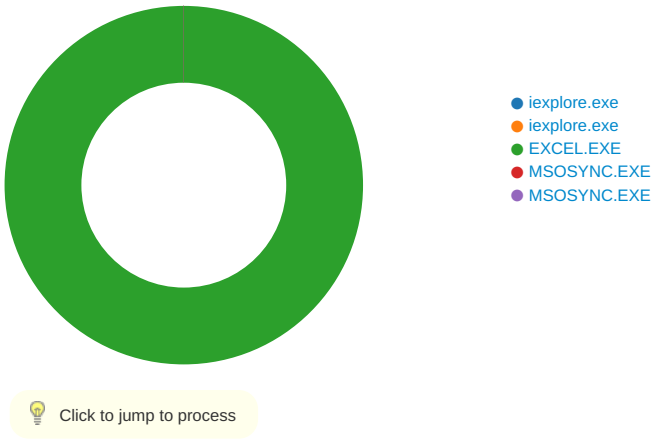
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49710	46.183.222.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:13:30.535327911 CET	3659	OUT	OPTIONS / HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Protocol Discovery Host: covid19vaccine.hopto.org Content-Length: 0 Connection: Keep-Alive
Mar 9, 2021 15:13:30.607413054 CET	3660	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:13:29 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: httpd/unix-directory
Mar 9, 2021 15:13:34.194197893 CET	3663	OUT	HEAD /new.xlsx HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: covid19vaccine.hopto.org Connection: Keep-Alive
Mar 9, 2021 15:13:34.268307924 CET	3663	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:13:32 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2 Last-Modified: Tue, 02 Mar 2021 09:12:03 GMT ETag: "279800-5bc8a20abf075" Accept-Ranges: bytes Content-Length: 2594816 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4868 Parent PID: 792

General

Start time:	15:13:10
Start date:	09/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f30c0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2844 Parent PID: 4868

General

Start time:	15:13:11
Start date:	09/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4868 CREDAT:17410 /prefetch:2
Imagebase:	0xa0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EXCEL.EXE PID: 384 Parent PID: 792

General

Start time:	15:13:23
Start date:	09/03/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' -Embedding
Imagebase:	0x210000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\58FD3802.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6503B7	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\58FD3802.tmp	0	524288	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 00 28 00 00 00 01 00 00 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fe ff ff ff 00 00 00 00 00 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 ff 07 00 00 80 08 00 00 f9 08 00 00 7a 09 00 00 fb 09 00 00 7c 0a 00 00 fd 0a 00 00 7e 0b 00 00 ff 0b 00 00 80 0c 00 00 f9 0c 00 00 7a 0d 00 00 fb 0d 00 00 7c 0e 00 00 fd 0e 00 00 7e 0f 00 00 ff 0f 00 00 80 10 00 00 f9 10 00 00 7a 11 00 00 fb 11 00 00 7c 12 00 00 fd 12 00 00 7e 13 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....(.............. ....z.....|.....~..... ....z.....|.....~..... .....z.....|.....~.....	success or wait	5	6503B7	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: MSOSYNC.EXE PID: 1368 Parent PID: 384

General

Start time:	15:13:28
Start date:	09/03/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe

Imagebase:	0xcc0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: MSOSYNC.EXE PID: 4456 Parent PID: 384

General

Start time:	15:13:29
Start date:	09/03/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0xcc0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly