ID: 367670
Sample Name: Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 23:11:31
Date: 11/03/2021
Version: 31.0.0 Emerald

Table of Contents

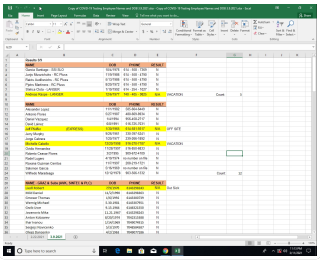
Analysis Report Copy of COVID-19 Testing Employee N…

Overview

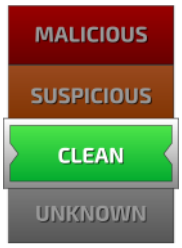
General Information

Sample Name:	Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx
Analysis ID:	367670
MD5:	8ea35bdf2130db8.
SHA1:	ef23db1561ad4a5.
SHA256:	f0ffa6cda325df3c..
Infos:	

Most interesting Screenshot:



Detection

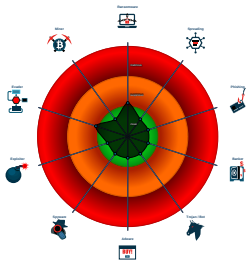


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5256 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

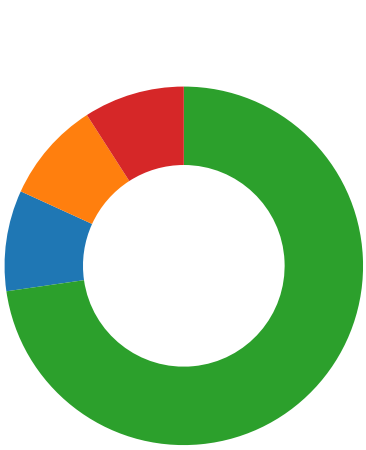
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



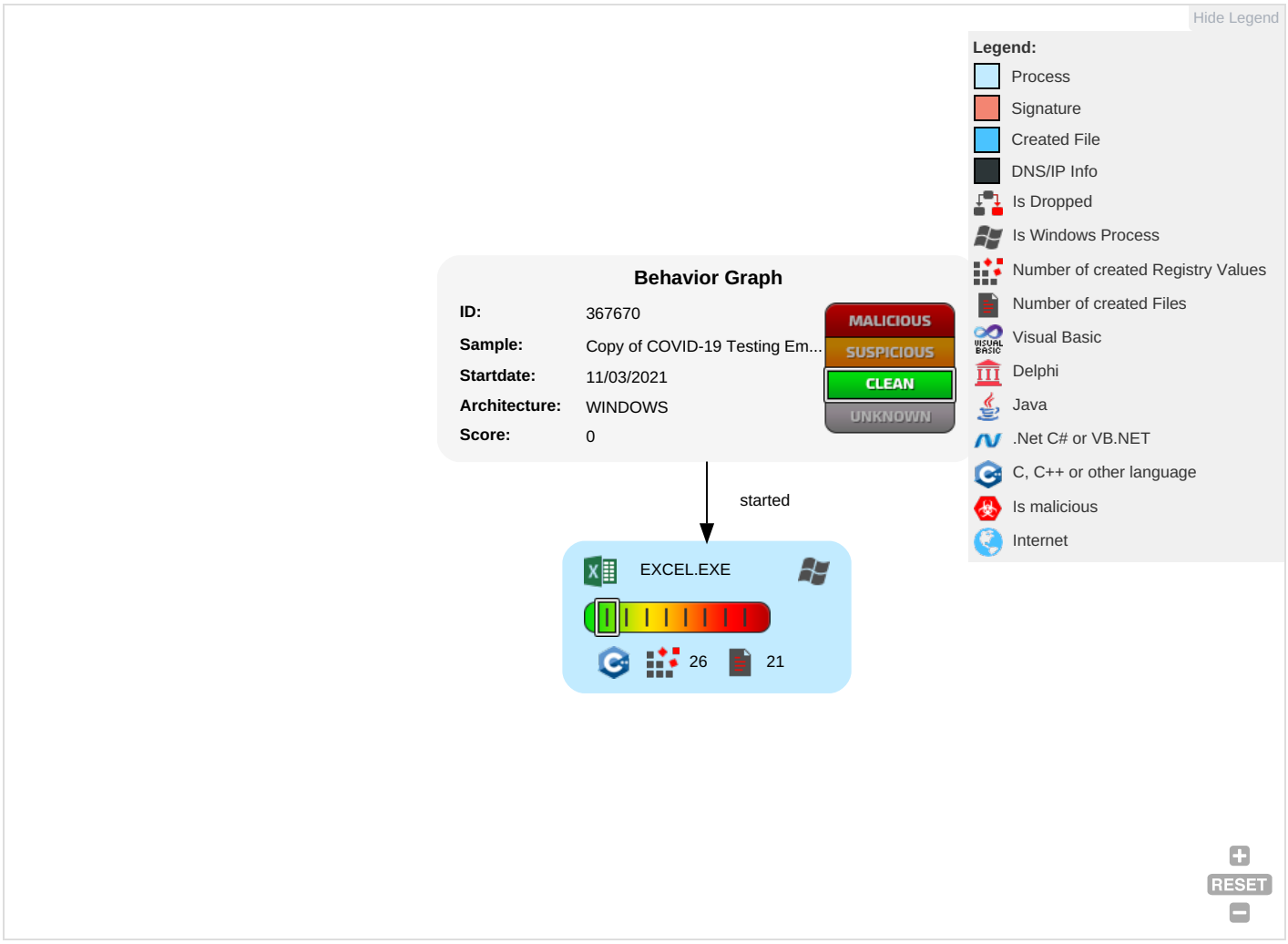
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

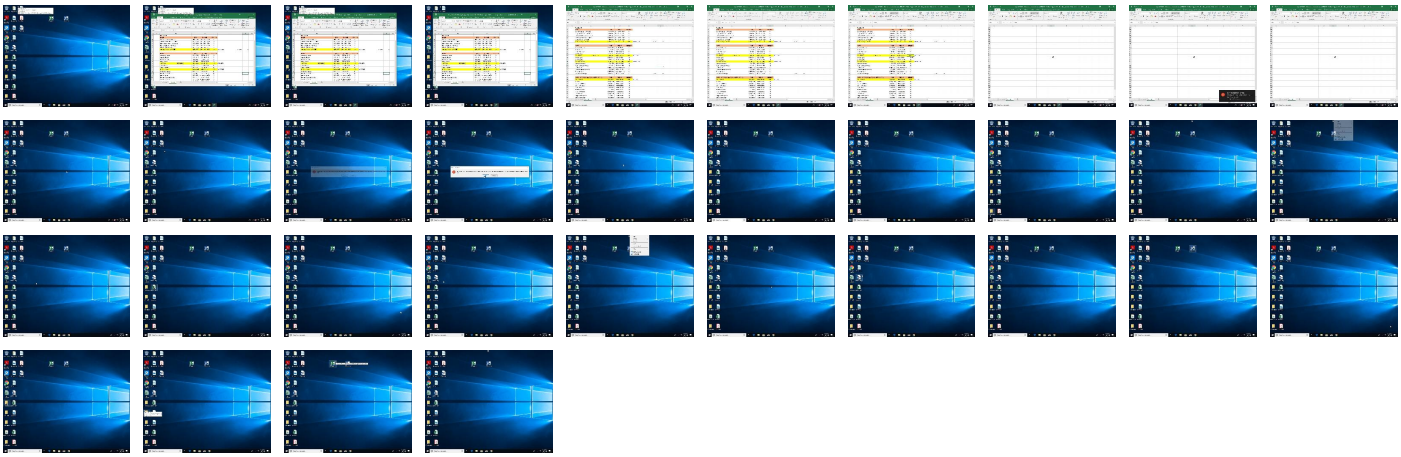
Behavior Graph

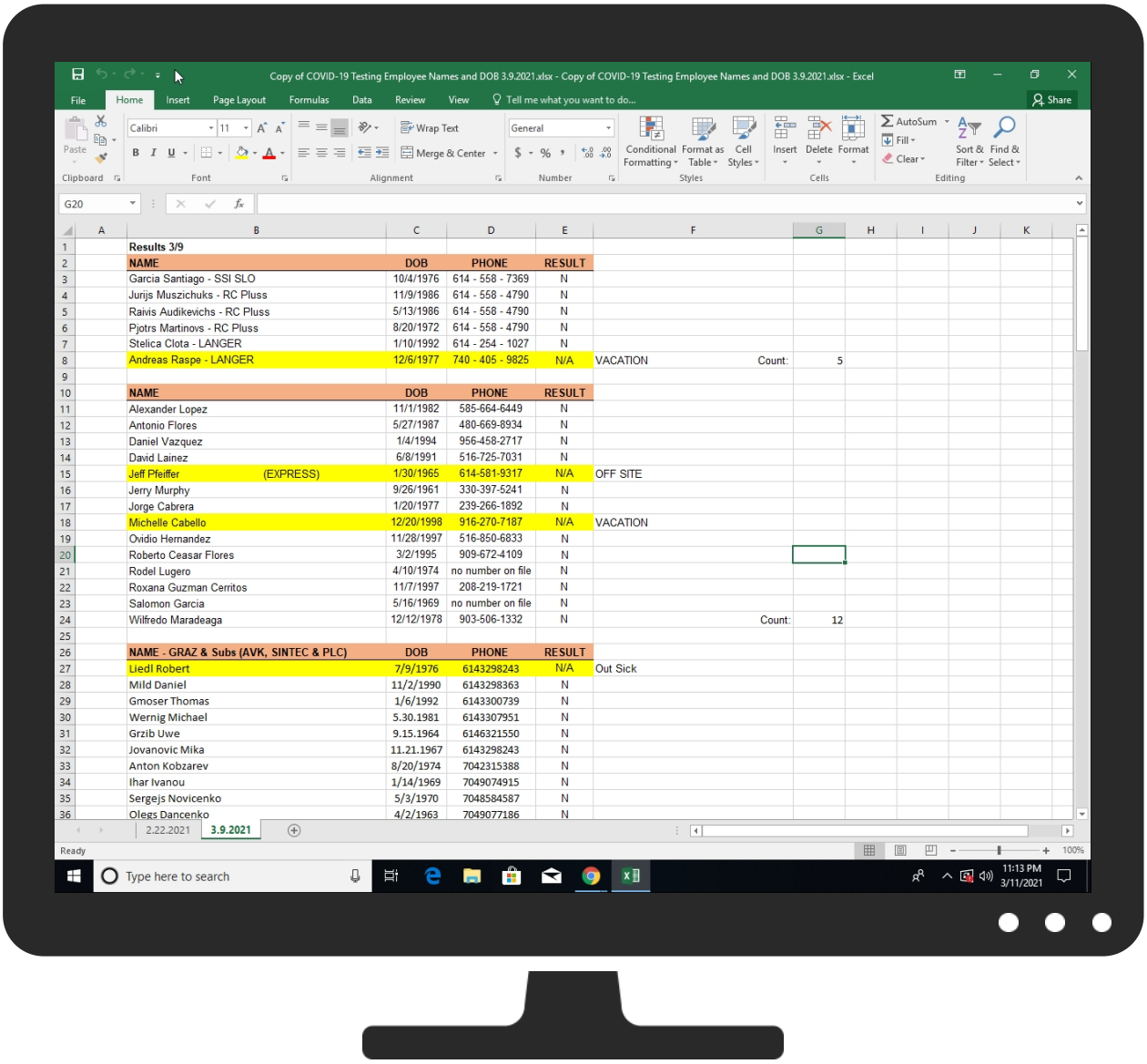


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
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://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%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	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	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
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://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	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://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://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://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	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://login.microsoftonline.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://shell.suite.office.com:1443	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://autodiscover-s.outlook.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://cdn.entity.	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://cortana.ai	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.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	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://api.aadrm.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://api.microsoftstream.com/api/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://cr.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://graph.ppe.windows.net	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://store.office.cn/addinstemplate	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.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=	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://web.microsoftstream.com/video/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://graph.windows.net	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://dataservice.o365filtering.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://ncus.contentsync.	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://weather.service.msn.com/data.aspx	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://apis.live.net/v5.0/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://management.azure.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://wus2.contentsync.	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://api.office.net	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://entitlement.diagnostics.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://outlook.office.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://templatelogging.office.com/client/log	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://outlook.office365.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://webshell.suite.office.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://management.azure.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://devnull.onenote.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://ncus.pagecontentsync.	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://messaging.office.com/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://augloop.office.com/v2	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://skyapi.live.net/Activity/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://dataservice.o365filtering.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false		high
http://https://staging.cortana.ai	30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	367670
Start date:	11.03.2021
Start time:	23:11:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	35
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:	CLEAN
Classification:	clean0.winXLSX@1/2@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.147.198.201, 52.255.188.83, 13.64.90.137, 52.109.76.68, 52.109.8.22, 52.109.12.23, 52.109.12.24, 13.107.5.88, 13.107.42.23, 51.104.144.132, 184.30.24.56, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.190.160.73, 20.190.160.2, 20.190.160.4, 20.190.160.136, 20.190.160.71, 20.190.160.67, 20.190.160.129, 20.190.160.134, 51.11.168.232, 51.104.136.2, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, login.live.com, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, l-0014.l-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, ams2.current.a.prd.aadg.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtReadVirtualMemory calls found.

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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\30DA7D9D-F2FB-48C1-B37D-CC74CE9E73CD	
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
Category:	dropped
Size (bytes):	132935
Entropy (8bit):	5.376872171380054
Encrypted:	false
SSDEEP:	1536:TcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdREh:bcQ9DQW+zUXiY
MD5:	0034D303EF90192987DF24F8CAF725BB
SHA1:	37A9B066F59326F9A83A0D7EF598B97EBDA9142D
SHA-256:	56E36C6D2F6CCEA96DF17E68EC16C3F83889B934EFD037ED39A64BF4933B240A
SHA-512:	D16594D13BBA9D2D7764E31C153EAEE1EDEDB8A7F39B838551C8C599C187321F32E43C879DF5DF7DCA121DAFB99CB012801F9BC4C92B440EC2AAD7B156EEA2A0
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="2021-03-11T22:12:20">.. Build: 16.0.13910.30528-->.. <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\Desktop\~$Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.610913327812838
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx
File size:	39748
MD5:	8ea35bdf2130db8f534db290aaceb9d0
SHA1:	ef23db1561ad4a51f3a3ba45e591a0ece7eff702
SHA256:	f0ffa6cda325df3c792de8f50f1fba7611c53731588d107bc40a8351d12d7da8
SHA512:	3d4a5cc53e70f13ec766424057d38f242576fabcfa98083f60a131d3396403d4ca0f35ff1a86dc2b18464e0232e06f6ca257a22f0cc7149e9165f70cdbd85e54
SSDEEP:	768:vU4jvnTUafBbF0OMYDBPfF5hYU7XDYehxPuGsyEj35Jv0as3FP:vU4zTR5PfF5N7XMsxPuGs5v8asl
File Content Preview:	PK..........!..B|{............[Content_Types].xml ...(..

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 11, 2021 23:12:09.128202915 CET	49199	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:09.177298069 CET	53	49199	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:10.068433046 CET	50620	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:10.117180109 CET	53	50620	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:10.932661057 CET	64938	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:10.984632969 CET	53	64938	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:11.774971008 CET	60152	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:11.838653088 CET	53	60152	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:12.579713106 CET	57544	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:12.631532907 CET	53	57544	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:13.852642059 CET	55984	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:13.901542902 CET	53	55984	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:17.325625896 CET	64185	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:17.383234024 CET	53	64185	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:19.636039019 CET	65110	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:19.686779022 CET	53	65110	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:20.554193974 CET	58361	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:20.615655899 CET	53	58361	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:21.064934015 CET	63492	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:21.125776052 CET	53	63492	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:21.165080070 CET	60831	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:21.216703892 CET	53	60831	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:22.069482088 CET	63492	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:22.130136013 CET	53	63492	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:22.799809933 CET	60100	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 11, 2021 23:12:22.848675966 CET	53	60100	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:23.084667921 CET	63492	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:23.142832994 CET	53	63492	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:23.581928968 CET	53195	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:23.633292913 CET	53	53195	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:24.533979893 CET	50141	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:24.596015930 CET	53	50141	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:25.084990978 CET	63492	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:25.144859076 CET	53	63492	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:25.678518057 CET	53023	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:25.730268955 CET	53	53023	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:26.496941090 CET	49563	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:26.546093941 CET	53	49563	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:27.435349941 CET	51352	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:27.487066031 CET	53	51352	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:28.380613089 CET	59349	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:28.432461023 CET	53	59349	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:29.085520029 CET	63492	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:29.142644882 CET	53	63492	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:29.565123081 CET	57084	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:29.613910913 CET	53	57084	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:38.613106012 CET	58722	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:38.613306046 CET	56596	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:38.613593102 CET	64101	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:38.662883043 CET	53	56596	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:38.662931919 CET	53	58722	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:38.663022041 CET	53	64101	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:41.699800014 CET	58823	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:41.748889923 CET	53	58823	8.8.8.8	192.168.2.3
Mar 11, 2021 23:12:47.999824047 CET	57568	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:12:48.074980021 CET	53	57568	8.8.8.8	192.168.2.3
Mar 11, 2021 23:13:00.075611115 CET	50540	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:13:00.147691965 CET	53	50540	8.8.8.8	192.168.2.3
Mar 11, 2021 23:13:03.727189064 CET	54366	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:13:03.788531065 CET	53	54366	8.8.8.8	192.168.2.3
Mar 11, 2021 23:13:16.540268898 CET	53034	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:13:16.589169979 CET	53	53034	8.8.8.8	192.168.2.3
Mar 11, 2021 23:13:20.437691927 CET	57762	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:13:20.496027946 CET	53	57762	8.8.8.8	192.168.2.3
Mar 11, 2021 23:13:51.038331032 CET	55435	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:13:51.088687897 CET	53	55435	8.8.8.8	192.168.2.3
Mar 11, 2021 23:13:53.266627073 CET	50713	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:13:53.325334072 CET	53	50713	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:04.056749105 CET	56132	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:04.117050886 CET	53	56132	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:04.662067890 CET	58987	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:04.716082096 CET	53	58987	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:05.212896109 CET	56579	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:05.264775038 CET	53	56579	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:05.733150005 CET	60633	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:05.794796944 CET	53	60633	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:07.141902924 CET	61292	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:07.199548960 CET	53	61292	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:09.054490089 CET	63619	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:09.111910105 CET	53	63619	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:09.535917044 CET	64938	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:09.596043110 CET	53	64938	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:10.297432899 CET	61946	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:10.349575043 CET	53	61946	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:11.195591927 CET	64910	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:11.247353077 CET	53	64910	8.8.8.8	192.168.2.3
Mar 11, 2021 23:15:11.721596956 CET	52123	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:15:11.778733969 CET	53	52123	8.8.8.8	192.168.2.3
Mar 11, 2021 23:17:03.938091040 CET	56130	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 11, 2021 23:17:03.987173080 CET	53	56130	8.8.8.8	192.168.2.3
Mar 11, 2021 23:17:04.588794947 CET	56338	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:17:04.659966946 CET	53	56338	8.8.8.8	192.168.2.3
Mar 11, 2021 23:17:08.171833038 CET	59420	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:17:08.239432096 CET	53	59420	8.8.8.8	192.168.2.3
Mar 11, 2021 23:17:11.290580034 CET	58784	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:17:11.339584112 CET	53	58784	8.8.8.8	192.168.2.3
Mar 11, 2021 23:17:11.668322086 CET	63978	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:17:11.734949112 CET	53	63978	8.8.8.8	192.168.2.3
Mar 11, 2021 23:19:23.236373901 CET	62938	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:19:23.288224936 CET	53	62938	8.8.8.8	192.168.2.3
Mar 11, 2021 23:19:57.424484968 CET	55708	53	192.168.2.3	8.8.8.8
Mar 11, 2021 23:19:57.491698027 CET	53	55708	8.8.8.8	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 11, 2021 23:17:03.987173080 CET	8.8.8.8	192.168.2.3	0x12d2	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 5256 Parent PID: 792

General

Start time:	23:12:18
Start date:	11/03/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xf0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	2551E4	WriteFile
C:\Users\user\Desktop\~$Copy of COVID-19 Testing Employee Names and DOB 3.9.2021.xlsx	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	255241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	1620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	16211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	16213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	16213B	RegSetValueExW

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

Disassembly